G DATA
SECURITY SOFTWARE

TRUST IN
GERMAN
SICHERHEIT

Inhaltsverzeichnis

1. Einführung....3
2. Installation....6
3. G Data ManagementServer....25
4. G Data Administrator....26
5. G Data WebAdministrator....114
6. G Data MobileAdministrator....116
7. G Data Security Client....121
8. G Data MailSecurity MailGateway....133
9. G Data MailSecurity Administrator....134
10. G Data Internet Security für Android....169
11. FAQ....180
12. Lizenzen....189

1. Einführung

In Zeiten der weltweiten Vernetzung und den daraus resultierenden massiven Sicherheitsrisiken, ist das Thema Virenschutz nicht länger nur für IT-Fachleute von Interesse. Es muss vielmehr im Rahmen eines umfassenden, unternehmensweiten Risikomanagements auf höchster Managementebene betrachtet werden. Ein durch Viren verursachter Ausfall des Computernetzwerks trifft ein Unternehmen an seiner empfindlichsten Stelle. Die Folgen: Stillstand lebenswichtiger Systeme, Verlust erfolgsrelevanter Daten, Ausfall wichtiger Kommunikationskanäle. Computerviren können einem Unternehmen Schäden zufügen, von denen es sich nie mehr erholt!

G Data bietet Ihnen High-End Virenschutz für Ihr gesamtes Netzwerk. Die führende Sicherheitsleistung der G Data-Produkte wird seit Jahren in zahlreichen Tests mit Traumnoten prämiert. Die G Data Business-Software setzt konsequent auf zentrale Konfiguration und Verwaltung sowie größtmögliche Automatisierung. Alle Clients, ob Workstation, Notebook oder Fileserver, werden zentral gesteuert. Sämtliche Client-Prozesse laufen transparent im Hintergrund ab. Automatische Internet-Updates sorgen im Ernstfall einer Virenattacke für extrem kurze Reaktionszeiten. Die zentrale Steuerung mit dem G Data ManagementServer ermöglicht Installation, Einstellungen, Updates, Fernsteuerung und Automatik für das gesamte Netzwerk. Das entlastet den Systemadministrator, spart Zeit und Kosten.

Wir wünschen Ihnen erfolgreiches und sicheres Arbeiten mit Ihrer G Data Business-Software.

Ihr G Data-Team

Versionsinformation
In dieser Dokumentation ist die Funktionalität aller G Data Business-Module beschrieben. Sollten Sie bei Ihrer installierten Software-Version ein Feature vermissen, können Sie über die G Data Premium Hotline bequem Informationen zum Upgrade Ihrer Software erhalten.

Copyright-Information
Copyright © 2014 G Data Software AG
Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2014 BitDefender SRL.
Engine B (CloseGap): © 2014 G Data Software AG
Engine B (Avast): © 2014 Alwil Software
OutbreakShield: © 2014 Commtouch Software Ltd.
Patch management: © 2014 Lumension Security, Inc.
DevCraft Complete: © 2014 Telerik, All Rights Reserved.
[G Data - 01.07.2014, 15:45]

1.1. G Data Business-Lösungen

Vom Endkunden über den Mittelstand bis hin zum Großunternehmen bietet G Data umfassenden Komplettschutz für jedes Netzwerk. Dank der neuesten Spitzentechnologie, genießen unsere Kunden höchstmögliche Sicherheit, beste Leistung in Verbindung mit optimaler Benutzerfreundlichkeit. Wählen Sie aus unseren

Softwarepaketen Ihre maßgeschneiderte Lösung:

	AntiVirus	ClientSecurity	EndpointProtection	SmallBusiness Security
AntiVirus	■	■	■	■
BankGuard	■	■	■	■
ReportManager	■	■	■	■
Mobile Device Management	■	■	■	■
Firewall		■	■	■
AntiSpam		■	■	■
PolicyManager			■	
MailSecurity / ClientBackup	□	□	□	■
PatchManagement	□	□	□	
Als Managed Service erhältlich			□	

■ Inklusive □ Optional

1.2. Hilfe-Dokumentation

Ausführliche Informationen zur Verwendung der Software finden Sie in der Programmhilfe, die Sie jederzeit über die Taste F1 kontextsensitiv öffnen können. Außerdem haben Sie die Möglichkeit, eine ausführliche PDF-Dokumentation im Downloadbereich der G Data Webseite herunterzuladen:

www.gdata.de

1.3. G Data Security Labs

Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Klicken Sie dazu im Bereich **Berichte** mit der rechten Maustaste auf einen Virusfund und wählen dort die Option **Quarantäne: An G Data Security Labs senden**. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.

Die Rücksende-Adresse für Antworten von der Internet-Ambulanz können Sie im Bereich **Optionen** > **Server-Einstellungen** > **E-Mail** definieren.

1.4. PremiumHotline

Die PremiumHotline für G Data Netzwerklizenzen steht allen registrierten Business-Kunden jederzeit zur Verfügung.

Telefon: +49 234 9762 901
Nutzen Sie eine Flatrate, so ist das Supportgespräch nach den Tarifbedingungen ohne zusätzliche Kosten.

E-Mail: **business-support@gdata.de**

Viele Fragen und Sachverhalte sind auch schon im Supportbereich der G Data Website beantwortet worden. Besuchen Sie uns unter:

www.gdata.de

Die Registriernummer finden Sie je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Überprüfen Sie vor Gesprächen mit der Hotline, wie Ihr Computer/Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- Die **Versionsnummern** des G Data Administrators und des G Data ManagementServers (diese finden Sie im Hilfe-Menü des G Data Administrators)
- Die **Registrierungsnummer** oder den **Benutzernamen** für das Internet-Update
- Die genaue Windows-Version (Client/Server)
- Zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)
- Eventuell auftretende Fehlermeldungen (inkl. Fehlercodes, sofern vorhanden) im genauen Wortlaut

Mit diesen Angaben wird das Gespräch mit den Support-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Wenn möglich, platzieren Sie das Telefon in der Nähe eines Rechners, auf dem der G Data Administrator installiert ist.

2. Installation

Starten Sie Windows und legen das G Data-Installationsmedium ein. Es öffnet sich automatisch ein Installationsfenster. Wenn Sie eine digital verteilte Version der Software erhalten haben, extrahieren Sie alle Dateien und starten Sie Setup.exe. Um die Installation auf anderen Maschinen zu erleichtern, können die extrahierten Dateien auf DVD gebrannt oder auf einen USB-Stick kopiert werden. Schließen Sie alle anderen Programme, bevor Sie mit der Installation der G Data Software beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die die G Data Software zur Installation benötigt. Nachdem Sie die Schaltfläche Installieren gedrückt haben, erscheint ein Bildschirm, in dem Sie auswählen können, welche der G Data Software-Komponenten Sie installieren wollen. Folgende Installationsmöglichkeiten stehen zur Verfügung:

G Data Setup
Wählen Sie die zu installierende Komponente.
G Data ManagementServer
Der ManagementServer kontrolliert und steuert alle Clients auf Workstations, Notebooks oder File-Servern und versorgt diese mit Updates der Virensignaturen. Die Installation beinhaltet den G Data Administrator.
G Data Bootmedium Wizard
Mit Hilfe des Bootmedium Wizards können Sie eine bootfähige CD zur Basisvirenanalyse erstellen. Dazu werden die aktuellen Virensignaturen verwendet.
G Data Administrator
Der Administrator ist die Steuerungssoftware für den ManagementServer. Er kann von einem beliebigen Rechner im Netz gestartet werden.
G Data WebAdministrator
Der WebAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Web-Browsers gestartet werden.
G Data Security Client
Die Client-Software stellt den Virenschutz für die Clients her und führt die Jobs vom ManagementServer ohne Benutzeroberfläche im Hintergrund aus.
G Data MobileAdministrator
Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden.
G Data InternetSecurity
Die InternetSecurity-Software schützt nicht vernetzte Rechner mit Internetzugang.
Schließen

- **G Data ManagementServer**: Als erstes sollte der G Data ManagementServer auf dem Computer installiert werden, der alle G Data - relevanten Einstellungen und Updates verwalten soll. Der G Data ManagementServer ist das Herzstück der G Data Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Mit der Installation des G Data ManagementServers wird automatisch auch die G Data Administrator-Software installiert, mit der der G Data ManagementServer gesteuert wird.
- **G Data Administrator**: Der G Data Administrator ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data - Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner installiert und gestartet werden, der übers Netzwerk mit dem G Data ManagementServer verbunden ist.
- **G Data Security Client**: Die Client-Software stellt den Virenschutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den G Data Administrator.

- **G Data InternetSecurity**: Wenn Sie die SmallBusiness-Versionen der G Data Software nutzen, steht Ihnen die G Data InternetSecurity als zusätzlicher autonomer Schutz für Rechner zur Verfügung, die nicht mit Ihrem Netzwerk verbunden sind, z.B. Notebooks von Außendienstmitarbeitern. Diese Software beinhaltet eine umfangreiche eigene Hilfedokumentation.
- **G Data Bootmedium Wizard**: Mit Hilfe des G Data Bootmedium Wizards können Sie eine bootfähige CD, DVD oder einen USB-Stick zur grundlegenden Überprüfung Ihres Rechners erstellen. Diese Überprüfung findet noch vor dem Start des installierten Betriebssystems statt. Dazu werden die aktuellen Virensignaturen verwendet.
- **G Data WebAdministrator**: Der G Data WebAdministrator ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden. Er kann auf diese Weise ein Ersatz für die Installation des G Data Administrators sein.
- **G Data MobileAdministrator**: Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden und bietet Ihnen grundlegende Administrationsfunktionen des G Data Administrators.
- **G Data MailSecurity**: Die G Data MailSecurity sichert - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr. Die G Data MailSecurity ist als optionales Modul verfügbar und steht auf einem eigenen Installationsmedium zur Verfügung.

2.1. Erste Schritte

Führen Sie bei akutem Virenverdacht auf den betroffenen Rechnern erst einen **boot scan** durch.

1. Installieren Sie den G Data ManagementServer auf Ihrem Server. Bei der Installation des G Data ManagementServers wird automatisch der **G Data Administrator** auf dem Server installiert. Mit diesem Programm kann der G Data ManagementServer gesteuert werden. Um den optimalen Schutz zu gewährleisten, sollte der Rechner immer erreichbar (eingeschaltet) sein und für das automatische Laden der Virensignaturen über einen Internetzugang verfügen. Eine Installation des G Data ManagementServers muss nicht auf einem Serverbetriebssystem erfolgen (siehe **Systemvoraussetzungen**).
2. Führen Sie nun die Online-Registrierung durch. Ohne eine Online-Registrierung können keine Aktualisierungen der Software und der Antivirensignaturen erfolgen.
3. Beim ersten Start des G Data Administrators auf dem Server startet der **Einrichtungsassistent**. Mit diesem kann die **Client-Software** auf den gewünschten Clients in Ihrem Netzwerk auch über eine Remote-Installation verteilt und eingespielt werden. Alle Einstellungen, die mit dem Einrichtungsassistenten vorgenommen werden, lassen sich auch nachträglich

ändern.

Sollten sich Probleme bei der Remote-Installation der Clients ergeben, kann die Client-Software auch über eine Active Directory Synchronisierung eingespielt werden oder lokal auf dem jeweiligen Client mit Hilfe des G Data-Installationsmediums oder einem selbst erstellten Client-Installationspaket installiert werden. Client-Installationspakete können auch über GPO/ Anmelde-Skripte verteilt werden. Damit der Server selbst vor Virenbefall geschützt ist, empfiehlt sich auch für den Server die Installation der Client-Software.

4. Nach erfolgter Einrichtung und Installation der Client-Software auf den angeschlossenen Maschinen kann der Virenschutz sowie die Internet-Updates der G Data Client- und Serversoftware zentral gesteuert werden. Der G Data Administrator bietet unter anderem Einstellungsmöglichkeiten für den Echtzeitschutz durch den G Data Wächter sowie die Möglichkeit, Scanaufträge zu definieren, die das Netzwerk regelmäßig auf Virenbefall untersuchen.

   Sollte es notwendig werden, ein Einstellungsproblem an einem Client vor Ort zu lösen, kann der G Data Administrator auf jedem Client innerhalb des Netzwerks installiert werden. Damit entfällt die Notwendigkeit, alle Einstellungen lokal am Server vorzunehmen. Sollte es notwendig werden eine kritische Situation innerhalb Ihre Netzwerk außerhalb Ihre Unternehmen zu lösen, kann der G Data WebAdministrator über jeden Desktop-Web-Browser verwendet werden. Mit dem G Data MobileAdministrator können Sie die Administration sogar unterwegs von Ihren Mobile-Web-Browser aus durchführen.

2.1.1. Systemvoraussetzungen

Folgende Mindestanforderungen werden an die Clients- bzw. Server gestellt:

Minimale Systemvoraussetzungen

G Data ManagementServer/G Data MailSecurity MailGateway

- Betriebssystem: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-Bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003
- Arbeitsspeicher: 1 GB

G Data Administrator/G Data WebAdministrator/G Data MailSecurity Administrator

- Betriebssystem: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-Bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 oder Windows Server 2003

G Data MobileAdministrator

- Betriebssystem: Windows 8, Windows 7, Windows Server 2012 oder Windows Server 2008 R2

G Data Security Client

- Betriebssystem: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-Bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 oder Linux-Kernel 2.6.25 oder höher
- Arbeitsspeicher: 1 GB

G Data Internet Security für Android

- Betriebssystem: Android 2.1 oder höher
- Freier Speicherplatz: 14 MB

G Data MailSecurity für Exchange (64-Bits Exchange-Plugin)

- Mail-Server: Microsoft Exchange Server 2013, Microsoft Exchange Server 2010 oder Microsoft Exchange Server 2007 SP1

Das G Data-System nutzt das TCP/IP-Protokoll zur Kommunikation von Client- und Server-Rechnern untereinander.

Empfohlene Systemvoraussetzungen

Bei der Verwendung von G Data ManagementServer/G Data MailSecurity MailGateway mit einer lokalen SQL-Datenbank oder anderen anspruchsvollen Anwendungen auf dem gleichen Rechner, gelten die folgenden empfohlenen Systemvoraussetzungen:

- Arbeitsspeicher: 4 GB
- CPU: multicore

2.1.2. Port-Konfiguration

Die G Data Produkte nutzen unterschiedliche TCP-Ports zur sicheren Kommunikation innerhalb Ihres Netzwerks. Bitte stellen Sie sicher, dass diese Ports in Ihrer Firewall entsprechend freigegeben sind:

Main-Server (MMS)

- Port 7161 (TCP): Kommunikation zwischen Clients und Subnet-Servern
- Port 7182 (TCP): Kommunikation mit dem G Data Administrator
- Port 7183 (TCP): Kommunikation mit mobilen Clients
- Port 7184 (TCP): Kommunikation mit mobilen Clients (Distribution der Installationsdateien für mobile Clients)

Subnet-Server

- Port 7161 (TCP): Kommunikation mit Clients und Subnet-Servern

Clients

- Port 7167 (TCP): Kommunikation mit (Subnet)-Servern
- Port 7169 (TCP): Kommunikation mit Clients (Peer-to-peer Update-Distribution)

MailSecurity MailGateway Server

- Port 7182 (TCP): Kommunikation mit G Data MailSecurity Administrator

MailSecurity Exchange-Plugin

- Port 7171 (TCP): Kommunikation mit G Data Administrator

Die Portnummern wurden für die G Data Software so ausgewählt, um Konflikte mit bestehenden Standardanwendungen zu vermeiden. Sollte es dennoch zu Port-Konflikten kommen, können Sie die Ports des G Data ManagementServers natürlich entsprechend ändern. Öffnen Sie dazu zuerst den Dienste-Manager (**Start**, **Ausführen**, *services.msc*) mit Administrator-Rechten und stoppen Sie den G Data ManagementServer Hintergrund-Task. Öffnen Sie nun im Installationsordner Ihres G Data Produktes (typischerweise C:\Program Files\G DATA\G DATA AntiVirus ManagementServer) die Datei gdmms.exe.config in einem Text-Editor (z.B. Notepad). Hinterlegen Sie Sie nun - falls notwendig - für die folgenden Einträge geänderte Portnummern:

- **AdminPort**: Geben Sie hier die gewünschte Portnummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7182).
- **ClientHttpsPort**: Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7183). In der Regel sollte der ClientHttpsPort-Wert nicht geändert werden, da mobile Clients keinen alternativen Port akzeptieren.
- **ClientHttpPort**: Geben Sie hier die gewünschte Proxy-Nummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7184).

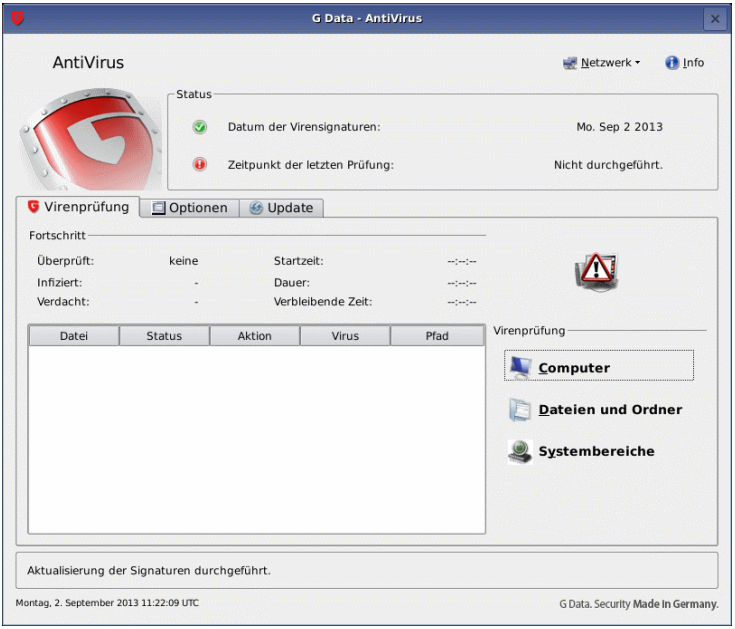
Wenn Sie die Werte für den ClientHttpPort oder den ClientHttpsPort ändern, müssen Sie die HTTP-Sicherheitskonfiguration für den jeweiligen Port neu initialisieren. Öffnen Sie dazu die Kommandozeile mit Administrator-Rechen und starten Sie *C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert*.

Führen Sie einen Neustart des G Data ManagementServers durch, nachdem Sie die Ports geändert haben. Bitte beachten Sie: Falls Sie den AdminPort geändert haben, müssen Sie bei jedem Einloggen beim G Data Administrator den geänderten Port angeben. Dies erfolgt in folgendem Format: *Servername:Port*.

2.1.3. G Data Bootmedium

Das G Data Bootmedium erlaubt eine Bekämpfung von Viren, die sich vor der Installation der Antivirensoftware auf dem Rechner eingenistet haben und möglicherweise die Installation der G Data Software unterbinden möchten. Dazu gibt es eine spezielle Programmversion der G Data AntiVirus, die schon vor dem Systemstart

ausgeführt werden kann.



1. **Mit dem Installationsmedium**: Legen Sie das G Data-Installationsmedium ein. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.
2. **Mit selbst erstelltem G Data Bootmedium**: Hierzu muss zunächst das Erstellungsprogramm für das G Data Bootmedium installiert werden. Dies muss auf einem System erfolgen, auf dem ein G Data Security Client mit aktuellen Signaturen installiert ist. Folgen Sie bitte nach der Installation den Anweisungen des **G Data Bootmedium Wizards**, um ein Bootmedium zu erzeugen.
3. Starten Sie den Computer neu. Es erscheint das Startmenü des G Data Bootmediums.
4. Wählen Sie mit den Pfeiltasten ihre Sprache und danach die Option **G Data AntiVirus**. Es wird nun ein Linux-Betriebssystem gestartet und es erscheint eine Spezialversion von G Data AntiVirus.

   Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G Data AntiVirus – Alternativ** aus.
5. Wenn Sie selbst ein G Data Bootmedium erstellt haben, sind die Virensignaturen auf dem Updatestand, den der G Data Security Client zum Zeitpunkt der Erstellung des Bootmediums geladen hat. Falls nötig, schlägt das Programm vor, die Virensignaturen zu aktualisieren. Klicken Sie hier auf **Ja** und führen Sie das Update durch. Stellen Sie sicher, dass Sie ihre Registriernummer oder Zugangsdaten eingegeben haben, damit das Update durchgeführt werden kann.

6. Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Computer** und Ihr Computer wird auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnertyp und Festplattengröße eine Stunde oder länger dauern.
7. Sollte die G Data Software Viren finden, entfernen Sie diese mit Hilfe der im Programm vorgeschlagenen Option. Nach einer erfolgreichen Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.
8. Nach Abschluss der Virenüberprüfung klicken Sie auf die Schließen-Schaltfläche (oben rechts in der Linux-Programmoberfläche) und wählen anschließend **Beenden** > **Herunterfahren** aus.
9. Entfernen Sie das G Data Bootmedium aus dem CD-Laufwerk bzw. dem USB-Port.
10. Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Betriebssystem. Die G Data Software kann nun auf einem virenfreien System installiert werden.

2.1.3.1. G Data Bootmedium Wizard

Um ein G Data Bootmedium zu erstellen, müssen Sie zunächst G Data Bootmedium Wizard installieren. Dies sollte auf einem System erfolgen, auf dem ein G Data Security Client mit aktuellen Virensignaturen läuft. Legen Sie das G Data-Installationsmedium ein und klicken Sie auf die **Installieren**-Schaltfläche. Wählen Sie nun **G Data Bootmedium Wizard** aus.

Bootmedium Wizard
Willkommen!
Der Bootmedium Wizard unterstützt Sie bei der Erstellung einer bootfähigen CD oder DVD. Außerdem können startfähige USB-Sticks erstellt werden.
Dieses Medium wird automatisch bei Systemstart geladen und prüft Ihren Rechner auf Schädlinge, ohne dass Ihr eigentliches Betriebssystem gestartet wird.
Details zur Verwendung des Bootmediums entnehmen Sie bitte der Anleitung.
< Back
Next >
Cancel

Nach Abschluss der Installation können Sie unter **Start** > **(Alle) Programme** > **G Data** > **G Data Bootmedium Wizard** mit einem Klick auf **G Data Bootmedium Wizard** assistentengestützt ein Bootmedium erzeugen. Bitte achten Sie darauf, ein Virensignatur-Update durchzuführen, damit das Bootmedium die neuesten Virensignaturen enthält. Danach können Sie das Bootmedium erzeugen, indem Sie dieses auf CD brennen, auf einem USB-Stick speichern oder als ISO-Image speichern. Das ISO-Image kann dann ggf. über das Netzwerk an die Clients distribuiert werden.

2.1.3.2. Boot-Option im BIOS einstellen

Sollte das System nicht von CD/DVD-ROM oder USB-Stick booten, kann es sein, dass diese Option erst eingestellt werden muss. Dies erfolgt im BIOS, einem System, das noch vor Ihrem Betriebssystem gestartet wird. Um hier Änderungen vorzunehmen, führen Sie folgende Schritte durch:

1. Schalten Sie den Computer aus.
2. Starten Sie Ihren Computer wieder. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **Entf**-Taste (manchmal auch die Taste **F2**- oder **F10**-Taste) drücken. Die Dokumentation des Rechnerherstellers liefert hierzu weitere Hinweise.
3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, entnehmen Sie der Dokumentation Ihres Mainboard-Herstellers. Im Ergebnis sollte die Bootreihenfolge **USB, CD/DVD-ROM, C:** lauten, d.h. USB-Sticks werden zum 1. Boot-Device, das CD/DVD-ROM-Laufwerk zum 2. Boot-Device und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum 3. Boot-Device.
4. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen Scan vor dem Systemstart.

2.2. Installation des G Data ManagementServers

Legen Sie das G Data-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente G Data ManagementServer aus. Schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen können. Lesen Sie sich nun die Lizenzvereinbarung zur Nutzung dieser Software durch. Wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken dann auf **Weiter**, wenn Sie den Vereinbarungen in dieser Form zustimmen.

Nach der Auswahl eines Installationsordners, kann der Server-Typ gewählt werden. Sie haben folgende Möglichkeiten:

- **Einen Main-Server installieren**: Bei einer Erstinstallation muss der G Data ManagementServer immer als Main-Server (Main-MMS) installiert werden. Der Main-Server stellt die zentrale Konfigurations- und Verwaltungsinstanz der netzwerkbasierten Virenschutz-Architektur dar. Die zu schützenden Rechner werden über den G Data ManagementServer mit den jeweils aktuellsten Virensignatur- und Programmupdates versorgt. Darüber hinaus werden sämtliche Client-Einstellungen zentral am G Data ManagementServer vorgenommen.
- **Einen Secondary-Server installieren**: Bei Verwendung einer SQL-Datenbank ist es möglich, einen zweiten Server (Secondary-MMS) zu betreiben, der auf die gleiche Datenbank wie der Hauptserver zugreift. Falls der Main-Server eine Stunde oder länger nicht erreichbar ist, werden die Clients sich automatisch mit dem Secondary-Server verbinden und von diesem Signaturupdates laden. Der

Wechsel zurück zum Hauptserver erfolgt, sobald dieser wieder verfügbar ist. Beide Server laden die Signaturupdates unabhängig voneinander und stellen so eine Ausfallsicherheit her.

- **Einen Subnet-Server installieren**: Bei großen Netzwerken (z.B. Firmenzentrale mit angeschlossenen Zweigstellen) kann es sinnvoll sein, einen G Data ManagementServer als Subnet-Server zu betreiben. Subnet-Server dienen der Entlastung des Netzwerks zwischen Clients und dem Main-MMS. Sie können in Netzwerken verwendet werden und verwalten dort die ihnen zugeordneten Clients. Die Subnet-Server bleiben funktionsfähig, auch wenn Main- oder Secondary-ManagementServer nicht erreichbar sind. Diese laden allerdings selbständig keine Virensignaturupdates. Geben Sie im Feld Name Main-Server den **Servernamen** ein, auf dem der Main-Server läuft.

  Eine Alternative zur Benutzung eines Subnet-Servers ist die Peer to Peer Updateverteilung. Durch die Aktivierung dieser Option wird die Netzauslastung zwischen Server und Client während der Updateverteilung stark reduziert. Bei einigen Netzwerken kann auf diese Weise die Installation eines Subnet-Servers überflüssig sein.

Wählen Sie nun eine Datenbank aus, die der G Data ManagementServer verwenden soll. Sie haben dabei die Möglichkeit, eine vorhandene SQL-Server-Instanz oder Microsoft SQL-Express zu verwenden. Wählen Sie die Express-Variante, wenn Sie G Data ManagementServer in einem Netzwerk mit weniger als 1000 Clients installieren. Die SQL-Server-Instanz-Variante bietet sich vor allem in größeren Netzwerken mit einer Client-Anzahl ab 1000 an. Falls Sie G Data ManagementServer auf einem Server installieren, auf dem sich schon eine SQL-Server-Express-Installation und eine ManagementServer-Datenbank befinden, wählen Sie die Instanz-Variante. Nach der Installation können Sie dann die Verbindung zum SQL Server (Express) mit Hilfe des Tools GdmmsConfig konfigurieren.

Während der Installation erfolgt die Produktaktivierung. Diese ermöglicht das Laden von Updates nach Beendigung der Installation.

- **Neuen Lizenzschlüssel eingeben**: Wenn Sie die G Data Software das erste Mal installieren, wählen Sie diese Option aus und geben anschließend die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor. Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgreicher Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich.

  Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

- **Zugangsdaten eingeben**: Wenn die G Data Software schon einmal installiert wurde, haben Sie Zugangsdaten (Benutzername & Passwort) erhalten. Um die G Data Software erneut zu installieren, geben Sie hier die Zugangsdaten an.
- **Später aktivieren**: Wenn Sie sich zunächst nur einen Überblick über die Software verschaffen möchten oder die Zugangsdaten für den Moment nicht greifbar sind, kann die Installation auch ohne Angabe von Daten installiert werden. Da auf diese Weise allerdings vom Programm keine Aktualisierungen aus dem Internet geladen werden, ist kein echter Schutz vor Schadsoftware gegeben. Nur mit tagesaktuellen Updates kann die G Data Software Ihren Computer effektiv schützen. Eine Nutzung der Software ohne Aktivierung schützt Sie nur unzureichend. Sie können Ihre Registrierungsnummer oder Ihre Zugangsdaten jederzeit nachträglich eingeben. Lesen Sie hierzu auch die Hinweise zur nachträglichen Aktivierung der G Data Software.

  Beachten Sie: wird die Software installiert, ohne sie zu aktivieren, sind nur die G Data AntiVirus-Komponenten verfügbar, selbst wenn Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder andere Module erworben haben. Die zusätzlichen Komponenten werden aktiviert und sind verfügbar, sobald die Software registriert wird.

Falls Sie sich für die Datenbankvariante SQL-Server-Instanz entschieden haben, erfolgt jetzt die Konfiguration des Datenbanktyps. Weitere Informationen hierzu finden Sie im Reference Guide. In der Regel reicht es, dieses Fenster durch Anklicken der **Schließen**-Schaltfläche zu schließen.

Nach der Installation des G Data ManagementServers ist dieser einsatzbereit. Ein Neustart des Servers könnte erforderlich sein. Der G Data ManagementServer wird bei jedem System(neu)start automatisch mitgestartet.

Um den G Data ManagementServer zu verwalten, können Sie unter **Start** > **(Alle) Programme** > **G Data Administrator** den Eintrag **G Data Administrator** auswählen und auf diese Weise das Administrationstool für den G Data ManagementServer starten.

2.3. Installation des G Data Administrators

Bei einer Installation des **G Data ManagementServers** wird automatisch auf demselben Rechner der G Data Administrator mitinstalliert. Eine nachträgliche Installation der Administratorsoftware auf dem G Data ManagementServer ist nicht erforderlich. Die Installation des G Data Administrators kann unabhängig von der Installation auf dem Server auch auf jedem Client-Rechner erfolgen. Auf diese Weise kann der G Data ManagementServer auch dezentral betreut werden.

Zur Installation des G Data Administrators auf einem Client-Rechner legen Sie das G Data-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente G Data Administrator aus.

Schließen Sie spätestens jetzt alle offenen Anwendungen im Windows-System, da

diese sonst zu Problemen bei der Installation führen können. Nach einem Klick auf **Weiter** wird die Installation fortgesetzt; folgen Sie dann den Installationsschritten, bei denen der Installationsassistent Sie unterstützt. Nach der Installation ist unter **Start** > **(Alle) Programme** > **G Data** > **G Data Administrator** der Eintrag **G Data Administrator** anwählbar.

2.4. Installation des G Data WebAdministrators

Legen Sie das G Data-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente G Data WebAdministrator durch einen Klick aus.

Die Installation des G Data WebAdministrators ist einfach und unkompliziert. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der WebAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z.B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von Systemvoraussetzungen - zusätzliche Software installiert werden:

- **Microsoft Internet Information Services (IIS)**: Da der WebAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der WebAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den WebAdministrator installieren.
- **Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration**: Vor der Installation des G Data WebAdministrators ist die Aktivierung der Windows-Funktion Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration erforderlich. Sollte diese Funktion nicht zur Verfügung stehen, wird die Installation des G Data WebAdministrators abgebrochen. Sie finden diesen Eintrag z.B. bei Windows Vista unter **Start** > **Systemsteuerung** > **Programme** > **Programme und Funktionen** > **Windows-Funktionen ein- oder ausschalten**. Hier können Sie den Eintrag unter **Internetinformationsdienste** > **Webverwaltungstools** > **Kompatibilität mit der IIS 6-Verwaltung** > **Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration** an- oder ausschalten. Außerdem müssen - soweit nicht schon geschehen - die WWW-Dienste aktiviert sein. Hierzu setzen Sie das Häkchen unter **Internetinformationsdienste** > **WWW-Dienste**. In Serverbetriebssystemen finden sich die entsprechenden Optionen im **Servermanager** bei **Rollen**.
- **Microsoft .NET Framework**: Der WebAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des WebAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.
- **Microsoft Silverlight**: Der G Data WebAdministrator benötigt Microsoft Silverlight. Falls dies bei der Installation nicht vorhanden ist, werden Sie beim ersten Start des G Data WebAdministrators darauf aufmerksam gemacht.

Nach der Installation steht Ihnen auf dem Desktop Ihres Computers das Symbol für den G Data WebAdministrator zur Verfügung. Darüber hinaus erhalten Sie einen Hyperlink, mit dem Sie den WebAdministrator über Ihren Browser aufrufen können.

Die Verwendung des WebAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS**.

2.5. Installation des G Data MobileAdministrators

Legen Sie das G Data-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente G Data MobileAdministrator durch einen Klick aus.

Die Installation des G Data MobileAdministrators ist der des WebAdministrators vergleichbar. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der MobileAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z.B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von Systemvoraussetzungen - zusätzliche Software installiert werden:

- **Microsoft Windows 7/Microsoft Windows Server 2008 R2**: MobileAdministrator benötigt mindestens Windows 7 oder Windows Server 2008 R2.
- **Microsoft Internet Information Services (IIS)**: Da der MobileAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der MobileAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den MobileAdministrator installieren.
- **Microsoft .NET Framework**: Der MobileAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des MobileAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.

Nach Beendigung der Installation stellt Ihnen der Installer einen Direktlink für den MobileAdministrator zur Verfügung, über den Sie diesen mit Ihrem Smartphone über einen Mobile Browser erreichen und bedienen können.

Die Verwendung des MobileAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS**.

2.6. Installation der G Data Security Clients

Zum Schutz und zur Verwaltung des Netzwerks sollte der G Data Security Client auf jedem Rechner im Netzwerk installiert sein. Je nach Einsatz-Szenario können Sie die Installation der Client-Software über eine **Remote-Installation** (über den G Data Administrator) oder über eine **lokale Installation** (per G Data-Installationsmedium oder ein Client-Installationspaket) durchführen. Darüber hinaus ist es auch empfehlenswert, den G Data Security Client auch auf dem Server zu installieren.

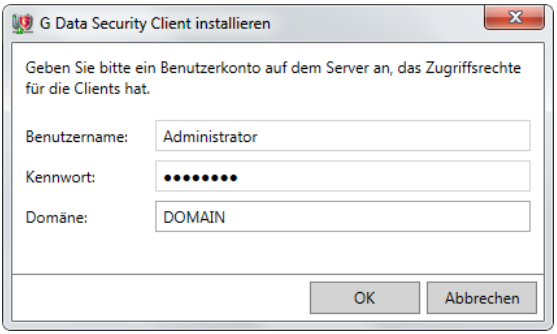
> Wenn Sie G Data Security Client auf einem Server installieren, sollen Sie sicherstellen dass keine Konflikte mit bestehenden Workflows entstehen. Zum Beispiel sollten Sie auf Database-Servern und E-Mail-Servern für manche Ordner und Dateien Scan- und Wächterausnahmen definieren. Weitere Informationen hierzu finden Sie im Reference Guide.

2.6.1. Remote-Installation

Der bequemste Weg, um die Client-Software auf den Clients zu installieren, ist die Remote-Installation über den G Data Administrator. Über den **Server-Einrichtungsassistent** können Sie automatisch den G Data Security Client auf allen im Netzwerk angeschlossenen Rechnern installieren.

Abgesehen von den erforderlichen **Port-Konfigurationen** sind folgende Voraussetzungen nötig, um eine Remote-Installation durchzuführen:

- Sofern eine Firewall verwendet wird, muss für die Datei gdmms.exe eine Ausnahme definiert sein.
- In einer Windows-Arbeitsgruppe muss die Option **Einfache Dateifreigabe** (Windows XP) oder **Freigabe-Assistent verwenden** (Windows Vista oder Windows 7) deaktiviert werden. Diese ist standardmäßig in allen Windows-Client-Installationen aktiviert und kann folgendermaßen deaktiviert werden: Öffnen Sie einen beliebigen Ordner im Windows-Explorer, klicken Sie dort auf **Extras** > **Ordneroptionen** > **Ansicht**, und deaktivieren Sie nun die Option **Freigabe-Assistent verwenden**.
- Die Benutzerkontensteuerung (UAC) sollte deaktiviert sein.
- Für die UNC-Freigaben C$ und Admin$ sollten Zugriffsberechtigungen verfügbar sein. Dies kann über ein lokales oder ein Domänen-Administrator-Konto erfolgen. Für die Remote-Client-Installation muss das Konto nicht unbedingt ein Kennwort haben. Allerdings muss der Zielrechner umkonfiguriert werden, um Netzwerkanmeldungen für Konten ohne Kennwort zu erlauben. Weitere Informationen hierzu finden Sie im Reference Guide. Für die Remote-Subnet-Server-Installation muss ein Kennwort gesetzt sein: ein leeres Kennwort-Feld ist nicht gestattet.
- In den Diensten muss der Remoteregistrierungsdienst aktiv sein.



Über den **Server-Einrichtungsassistenten**, der automatisch beim ersten Start des G Data Administrator aufgerufen wird, erhalten Sie einen Überblick über alle in Ihrem Netzwerk angemeldeten Computer. Darüber hinaus können Sie manuell weitere Computer per Namenseingabe hinzufügen und aktivieren. Nun können Sie den G Data Security Client einfach dadurch auf diesen Rechnern installieren, indem Sie einen Rechtsklick durchführen und in dem erscheinenden Kontextmenü **G Data Security Client installieren** auswählen. Nun erscheint ein Eingabefenster, in dem Sie **Benutzername**, **Kennwort** und **Domäne** mit Zugriffsrechten auf den Clients eingeben können. Nach Auswahl der Anzeigesprache werden Sie gefragt, ob Sie mit dem Client zugleich die **G Data Firewall** auf dem jeweiligen Client mit installieren möchten. Die Firewall steht Ihnen nur bei den Software-Versionen G Data ClientSecurity, G Data EndpointProtection, and G Data SmallBusiness Security zur Verfügung. Damit Sie den Status der Remote-Installation beobachten können, öffnet sich automatisch die **Installationsübersicht**. Nach einer erfolgreichen Installation der Software muss der Client-Rechner neu gestartet werden.

> Wenn Sie die **Active Directory Integration** nutzen, können Sie die Client-Software auch automatisch auf neu ins Netzwerk eingebundene Rechner installieren.

Die Remote-Installation kann auf zwei verschiedene Arten erfolgen. Wenn der Client die notwendigen Voraussetzungen erfüllt, können die Installationsdaten direkt vom Server aus überspielt und entsprechende Änderungen in der Registry vorgenommen werden. Wenn der Server nur Zugriff auf die Festplatte des Client-Rechners und nicht auf die Registry hat oder andere Systemvoraussetzungen nicht erfüllt sind, dann wird das Setup-Programm auf den Client kopiert und die Installation wird automatisch beim nächsten Neustart des Computers gestartet.

Wenn die Client-Software nicht über die Remote-Installation installiert werden kann, haben Sie darüber hinaus die Möglichkeit, die Client-Software lokal über das G Data-Installationsmedium oder das Client-Installationspaket durchzuführen. Ein Client-Installationspaket kann auch über logon scripts/group policy objects verteilt werden.

2.6.2. Lokale Installation

Wenn eine **Remote-Installation** nicht möglich ist, können Sie den G Data Security Client auch direkt manuell auf den Clients installieren. Sie können entweder das G Data-Installationsmedium dazu verwenden die Client-Software direkt auf dem Client zu installieren, oder ein Installationspaket zu erzeugen, welches dann die Installation im Hintergrund durchführt (ideal für die Distribution der Software über Login-Skripts).

2.6.2.1. G Data Installationsmedium

Zur lokalen Installation des Clients auf einem Client-Rechner legen Sie das G Data-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente G Data Security Client aus.

Geben Sie im Verlauf der Installation den Servernamen oder die IP-Adresse des Servers ein, auf dem der G Data ManagementServer installiert ist. Die Angabe des Servernamens ist notwendig, damit der Client über das Netzwerk mit dem Server in Kontakt treten kann.

2.6.2.2. Installationspaket

Das Paket ist eine einzelne ausführbare Datei (GDClientPck.exe), mit der ein neuer Client ohne weitere Benutzerinteraktion auf einem zu schützenden Rechner installiert werden kann. Das Installationspaket eignet sich beispielsweise dazu, den Client via Login-Script auf allen Rechnern einer Domäne zu verteilen oder dieses direkt lokal zu installieren. Das Paket enthält immer die auf dem Server aktuelle Client-Version.

Um ein Installationspaket zu erstellen, starten Sie den G Data Administrator. Im Menü **Organisation** wählen Sie bitte die Option **G Data Security Client Installationspaket erstellen**. Nun werden Sie aufgefordert, den ManagementServer auszuwählen, an welchem der Client sich registrieren soll und die Installationssprache. Nach der Auswahl eines Speicherortes erstellt der G Data Administrator nun ein Installationspaket im Hintergrund. Es ist unbedingt erforderlich, das Installationspaket auf den Zielrechner zu kopieren und dort mit Administrator-Rechten zu starten. Nun wird der G Data Security Client ohne weitere Benutzerinteraktion installiert.

2.6.3. Installation von Linux-Clients

Der Linux-Client kann (ebenso wie die Windows-Clients) in die Infrastruktur des G Data ManagementServers eingebunden und zentral über die G Data Administrator-Software gesteuert und mit Signaturupdates versorgt werden. Analog zu den Windows-Clients wird auch bei Linux-Clients ein Dateisystemwächter mit einer grafischen Benutzeroberfläche eingerichtet, die sich in der Funktionalität an der Windows-Version orientiert. Für Linux-Rechner, die als Fileserver arbeiten und verschiedenen Clients Windows-Freigaben (über das SMB-Protokoll) zur Verfügung stellen, kann hierzu ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem

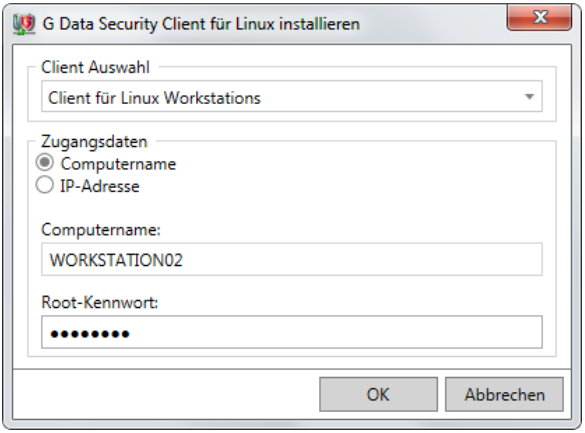
Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom Samba-Server auf die Windows-Clients (und umgekehrt) gelangen kann.

> Für den Workstation-Client ist eine Kernel-Version größer gleich 2.6.25 erforderlich, dies ist z.B. bei Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 und anderen aktuellen Distributionen der Fall. Bei anderen Distributionen ist im Einzelfall eine Anpassung erforderlich. Der Fileserver-Client lässt sich auf allen gängigen Distributionen verwenden.

2.6.3.1. Remote-Installation

Um die Software auf dem Linux-Client zu installieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Aufgabenbereich Clients im Menü **Clients** den Befehl **G Data Security Client für Linux installieren** aus. Nun erscheint ein Dialogfenster über das Sie den Client definieren können, auf den die Client-Software kopiert werden soll. Der Rechner muss dazu im Netzwerk bekannt sein.
2. Verwenden Sie die Auswahl **Computername**, wenn auf dem Client-Rechner ein Samba-Dienst installiert ist oder wenn der Rechner im Namesserver des Netzwerkes registriert ist. Sollte der Name des Rechners nicht bekannt sein, verwenden Sie die **IP-Adresse** des Rechners.
3. Geben Sie nun das **Root-Kennwort** des Rechners ein. Für eine Remote-Installation muss ein Root-Kennwort vergeben sein. Standardmäßig ist dies unter einigen Distributionen (z.B.) Ubuntu nicht der Fall.
4. Drücken Sie nun auf die **OK**-Schaltfläche. Der Installationsvorgang wird in der **Installationsübersicht** gezeigt.



2.6.3.2. Lokale Installation

Im Verzeichnis \Setup\LinuxClient auf dem G Data-Installationsmedium finden Sie die folgende Dateien

- **installer.bin** (Installer für den Linux-Client)
- **uninstaller.sh** (Uninstaller für den Linux-Client)

Sie können diese Dateien auf den Client-Rechner kopieren und zur Installation der Client-Software die entsprechende Datei starten. Zusätzlich finden Sie auf dem G Data-Installationsmedium noch eine Datei mit den Virensignaturen. Da die Software nach der Installation aber automatisch die neuesten Virensignaturen vom Server bezieht, ist die Installation dieser Datei fakultativ:

- **signatures.tar** (Archiv mit Virensignaturen)

2.7. Installation der G Data MailSecurity

Die Konfigurationsart der MailSecurity ist abhängig von dem Mail-Server, der im Netzwerk verwendet wird. In Netzwerken, in denen ein Microsoft Exchange Server 2007 SP1/2010/2013 benutzt wird, kann MailSecurity als Exchange-Plugin installiert werden. Die MailSecurity für Exchange meldet sich dann bei einem (lokalen) ManagementServer an und kann vom G Data Administrator verwaltet werden. Die selbständige Gateway-Lösung MailSecurity MailGateway kann mit allen Mail-Servern kombiniert werden. Diese wird vom G Data MailSecurity Administrator verwaltet.

2.7.1. Als Exchange-Plugin

Zur Installation der MailSecurity für Exchange legen Sie das G Data MailSecurity-Installationsmedium ein und drücken die Schaltfläche **Installieren**. Wählen Sie anschließend unter **Microsoft Exchange AntiVirus Plug-In** die Komponente **MailSecurity (Exchange)** aus und folgen Sie den Hinweisen des Installations-Assistenten.

Der Installations-Assistent der MailSecurity für Exchange fügt Microsoft Exchange Server 2007 SP1/2010/2013 ein Plugin hinzu. Das Plugin wird über den G Data ManagementServer gesteuert. Falls es schon einen ManagementServer im Netzwerk geben sollte, geben Sie während der Installation den Servernamen ein. Alternativ konfiguriert der Installations-Assistent eine lokale ManagementServer-Installation. Das Exchange-Plugin registriert sich automatisch beim lokalen ManagementServer, bzw. beim Netzwerk-ManagementServer. Falls der Installations-Assistent eine lokale ManagementServer-Installation konfiguriert, wird auch der G Data Administrator installiert. Die Funktionen sind identisch mit dem normalen G Data Administrator, jedoch stehen Einstellungen, die nicht zu MailSecurity für Exchange zutreffen, nicht zur Verfügung. Falls Sie eine bereits vorhandene ManagementServer-Installation benutzen, kann auch der bereits vorhandene G Data Administrator benutzt werden. Die Einstellungen für MailSecurity für Exchange finden Sie im G Data Administrator auf der Registerkarte **Exchange-Einstellungen**.

2.7.2. Als Gateway

G Data MailSecurity MailGateway kann auf einem dedizierten Server oder auf dem bestehenden Mail-Server installiert werden. Bei der Installation sind verschiedene Konfigurationen möglich - je nachdem, wo im Netzwerk die Installation erfolgt. Generell sollte sich das Gateway am besten direkt hinter Ihrer Netzwerk-Firewall befinden (soweit vorhanden), d.h. dass der SMTP/POP3-Datenstrom aus dem Internet über die Firewall direkt zum MailGateway geleitet und von dort weiter verteilt wird.

Zur Installation des MailGateways legen Sie das MailSecurity-Installationsmedium ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend unter **Mail Gateway** die Komponente **MailSecurity** aus und folgen Sie den Hinweisen des Installations-Assistenten.

Wenn Sie die Komponenten für die statistische Auswertung installieren, bekommt der G Data MailSecurity Administrator im **Status**-Bereich eine **Statistik**-Schaltfläche hinzugefügt. Hierüber können Sie sich statistische Informationen über den Mailserver anzeigen lassen. Die Anzeige dieser Statistik kann über **Optionen** > **Logging** konfiguriert werden.

In allen Fällen sollten direkt nach der Installation mehrere Optionen (IP-Adressen, Ports) konfiguriert werden, sowohl auf dem Rechner, auf dem MailGateway installiert wurde, als auch auf dem Mail-Server. Beispielhafte Port-Konfigurationen für verschiedene Einsatzszenarien finden Sie im Reference Guide.

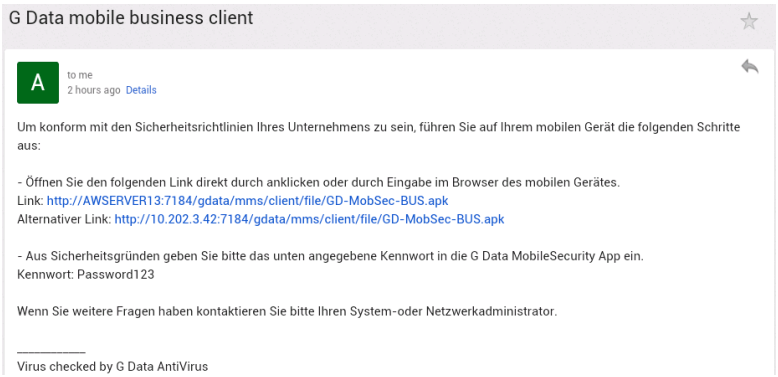
Je nachdem, wie Ihr Netzwerk aufgebaut ist, kann MailGateway an verschiedenen Knotenpunkten zugreifen, um Mails auf Virenbefall und Spam zu überprüfen:

- Wenn Sie Ihre Mails über einen externen Server als POP3-Mails bekommen, kann MailGateway eingreifen, um die POP3-Mails vor dem Öffnen durch den Empfänger auf Virenbefall zu überprüfen. Hierzu steht Ihnen die Funktion **Optionen** > **Eingehend (POP3)** zur Verfügung.
- Wenn Sie im Netzwerk einen SMTP-Server verwenden, kann MailGateway eingehende Mails schon überprüfen, bevor sie den Mail-Server erreichen. Hierzu steht Ihnen die Funktion **Optionen** > **Eingehend (SMTP)** zur Verfügung.
- MailGateway kann auch all Ihre ausgehenden Mails vor dem Versand auf Virenbefall überprüfen. Hier steht Ihnen die Funktion **Optionen** > **Ausgehend (SMTP)** zur Verfügung.

2.8. Installation der G Data Internet Security für Android

Um von den Möglichkeiten des G Data Mobile Device Management Gebrauch zu machen, können Sie eine auf Business-Belange ausgelegte Spezialversion der G Data Internet Security auf Ihren Android-Geräten installieren. Der G Data Administrator bietet

dabei Installationsmöglichkeiten für mobile Clients im Clientauswahlbereich. Klicken Sie auf die Schaltfläche **Installationslink an mobile Clients senden**, um eine Mail an die betreffenden Android-Geräte zu versenden. In dieser Mail befindet sich ein Download-Link für die Internet Security App. Sie können den Versand direkt an mehrere Mail-Adressen durchführen, in dem Sie diese - getrennt durch Zeilenumbruch oder Komma - eingeben. Wenn Sie bis jetzt noch kein Passwort eingegeben haben, können Sie es im Bereich **Server-Einstellungen** unter **Mobile** > **Authentifizierung für mobile Clients nachholen**.


G Data mobile business client
A
to me
2 hours ago Details
Um konform mit den Sicherheitsrichtlinien Ihres Unternehmens zu sein, führen Sie auf Ihrem mobilen Gerät die folgenden Schritte aus:
- Öffnen Sie den folgenden Link direkt durch anklicken oder durch Eingabe im Browser des mobilen Gerätes.
Link: http://AWSERVER13:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
Alternativer Link: http://10.202.3.42:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
- Aus Sicherheitsgründen geben Sie bitte das unten angegebene Kennwort in die G Data MobileSecurity App ein.
Kennwort: Password123
Wenn Sie weitere Fragen haben kontaktieren Sie bitte Ihren System-oder Netzwerkadministrator.
Virus checked by G Data AntiVirus

Nach dem Versand können Sie oder Ihre Mitarbeiter die Mail auf dem mobilen Gerät öffnen und durch Antippen des Download-Links die APK-Datei installieren. Bitte beachten Sie, dass die Option **Unbekannte Herkunft (Installation von Nicht-Market-Apps zulassen)** aktiviert sein muss, damit die Datei installiert werden kann. Diese Option finden Sie normalerweise im Android-System-Menü unter **Einstellungen** > **Sicherheit** > **Geräteverwaltung**.

Nach dem Öffnen der APK-Datei und dem Bestätigen der benötigten Berechtigungen wird die G Data Internet Security installiert und kann aus dem Android-App-Menü heraus gestartet werden. Über die **Einstellungen**-Schaltfläche können Sie nun die Fernadministration erlauben. Wählen Sie hierzu den Eintrag **Fernadministration gestatten** aus und und geben Sie den Namen oder die IP-Adresse des ManagementServers unter **Serveradresse** ein. Unter **Gerätename** können Sie nun für das Android-Gerät einen Namen zuweisen, unter dem dieses im G Data Administrator ermittelt werden kann. Bei **Passwort** sollten Sie das Passwort eintragen, welches Sie auch beim G Data Administrator eingetragen haben (dieses Passwort ist auch in der Mail angegeben, die Ihnen mit dem Download-Link ans Android-Gerät geschickt wurde).

Das Gerät wird nun neben den anderen Clients im **Clients**-Bereich des G Data Administrators angezeigt und kann von dort aus administriert werden. Sollte das Gerät nicht automatisch in dieser Liste erscheinen, rebooten Sie bitte das Gerät, um das Einchecken beim G Data ManagementServer zu forcieren.

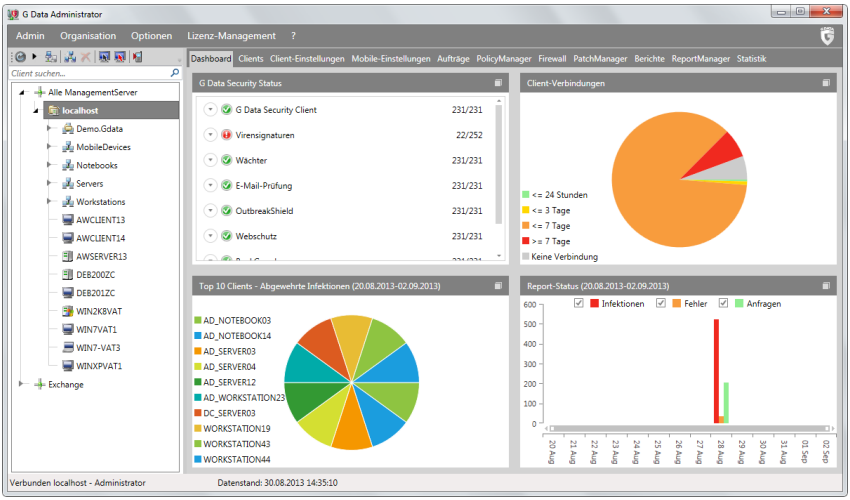
3. G Data ManagementServer

Der G Data ManagementServer ist das Herzstück der G Data-Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Zur Kommunikation mit den Clients nutzt der G Data ManagementServer das TCP/IP-Protokoll. Für Clients, die vorrübergehend keine Verbindung zum G Data ManagementServer haben, werden die Jobs automatisch gesammelt und beim nächsten Kontakt zwischen G Data Security Client und G Data ManagementServer synchronisiert. Der G Data ManagementServer verfügt über einen zentralen Quarantäne-Ordner. In diesem können verdächtige Dateien verschlüsselt sichergestellt, gelöscht, desinfiziert oder gegebenenfalls an die G Data SecurityLabs weitergeleitet werden. Der G Data ManagementServer wird über den **G Data Administrator** gesteuert.

> Wenn Sie den G Data Administrator beenden, bleibt der G Data ManagementServer weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen für die Clients eingestellt wurden.

4. G Data Administrator

Der G Data Administrator ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data-Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner innerhalb des Netzwerkes installiert und gestartet werden. Im G Data Administrator lassen sich Scanaufträge und Wächterfunktionen sowie Änderungen von Einstellungen vornehmen. Automatische Clientinstallationen, Software- und Virensignaturupdates, werden ebenfalls dort festgelegt.



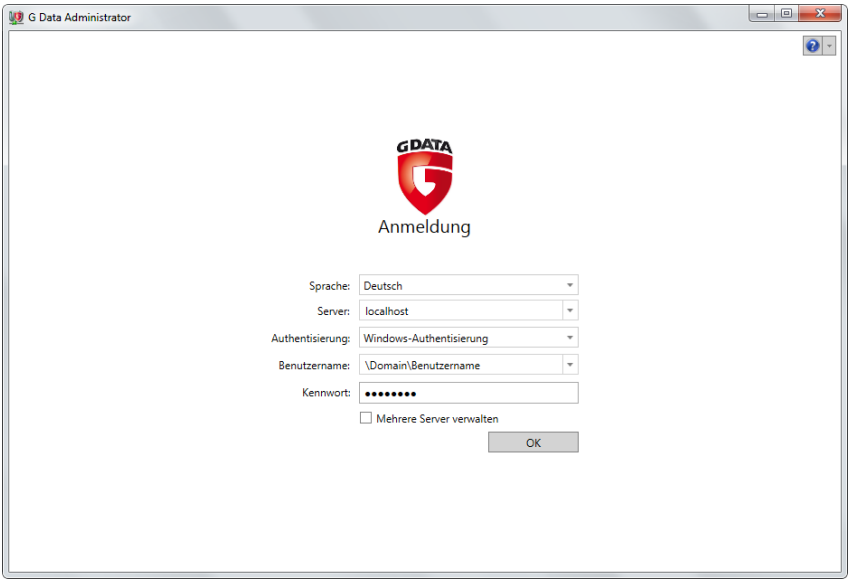
Die Oberfläche des G Data Administrators ist in folgende Bereiche untergliedert:

- Der links befindliche **Clientauswahlbereich** zeigt alle Clients, die bereits aktiviert sind und auf welchen die G Data Client Software schon installiert ist oder installiert werden kann.
- Rechts davon kann über Karteireiter in die jeweiligen Aufgabenbereiche gewechselt werden. Der Inhalt des Aufgabenbereiches bezieht sich normalerweise auf den im Clientauswahlbereich markierten Computer bzw. auf die markierte Gruppe von Clients.
- Oberhalb dieser Spalten finden Sie eine Menüleiste für globale Funktionen, die in allen Aufgabenbereichen verwendet werden können, sowie Sonderfunktionen für ausgewählte Aufgabenbereiche.

Bei der Administration von Linux-Clients, die auf Samba-Servern installiert sind, sind Funktionen, die z.B. den Umgang mit E-Mails beinhalten, gesperrt, da diese im Kontext eines Fileservers nicht notwendig sind. Funktionen, die für Linux-Clients nicht einstellbar sind, werden durch ein rotes Ausrufezeichen vor der jeweiligen Funktion markiert.

4.1. Starten des G Data Administrators

Das Administrator-Tool zur Steuerung des G Data ManagementServers wird mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start** > **(Alle) Programme** > **G Data** > **G Data Administrator** des Startmenüs aufgerufen.



Beim Starten des G Data Administrators werden Sie nach dem **Server**, **Authentisierung**, **Benutzername** und **Kennwort** gefragt. Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der G Data ManagementServer installiert wurde. Wählen Sie nun Ihre Authentisierung aus:

- **Windows-Authentisierung**: Wenn Sie diese Authentisierungsvariante wählen, können Sie sich mit dem Benutzernamen und Passwort Ihres Windows-Administrator-Zugangs auf dem G Data ManagementServer einloggen.
- **Integrierte Authentisierung**: Sie können sich über ein im G Data ManagementServer integriertes Authentisierungssystem einloggen. Integrierte Accounts können über die Funktion **Benutzerverwaltung** angelegt werden.

Klicken Sie auf den Pfeil neben dem Fragezeichen um ein Menü mit weiteren Optionen zu öffnen. **Über G Data Administrator** zeigt Versionsinformationen. **Einstellungen zurücksetzen** ermöglicht Ihnen die Ansichtseinstellungen des G Data Administrators zurück zu setzen (z.B. Fenstergröße).

4.2. G Data Administrator konfigurieren

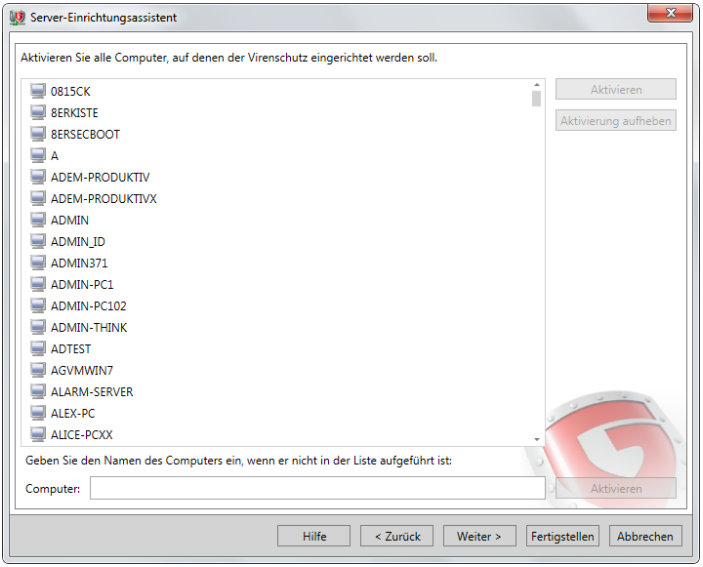
Bevor die ersten Clients konfiguriert werden, empfiehlt es sich, die wichtigsten Einstellungen des G Data Administrator und G Data ManagementServer zu überprüfen und für das eigene Netzwerk zu optimieren. Dies beinhaltet administrative Aufgaben, wie den Server-Einrichtungsassistent, die Benutzerverwaltung und Server-Einstellungen wie z.B. Alarmmeldungen, Internet-Update und E-Mail Einstellungen.

4.2.1. Administrative Einstellungen

Der Bereich Administrative Einstellungen kann über das **Admin**-Menü in der G Data Administrator-Menüleiste ausgewählt werden. Die meisten der hier aufgelisteten Tasks sollte mindestens einmal durchgeführt werden, bevor eine weitere Konfiguration und Bereitstellung erfolgt.

4.2.1.1. Server-Einrichtungsassistent

Mit dem Einrichtungsassistenten lassen sich im Netzwerk die Clients auswählen und aktivieren, für die die G Data Software den Virenschutz bereitstellen soll. Der Einrichtungsassistent wird automatisch beim ersten Starten des G Data Administrators ausgeführt, kann aber auch nachträglich jederzeit über das **Admin**-Menü erneut durchgeführt werden.



Zunächst müssen alle Clients, die von der G Data Software überwacht werden sollen, aktiviert werden. Die zu aktivierenden Clients müssen zunächst markiert und mit einem Klick auf **Aktivieren** aktiviert werden. Eventuell sind einige Computer nicht in der Liste enthalten (z.B. weil die betreffenden Rechner lange nicht eingeschaltet waren

oder keine Datei- bzw. Druckerfreigabe eingerichtet haben). Zum Aktivieren dieser Clients wird im Eingabefeld **Computer** der Name des Rechners eingegeben. Nach einem Klick auf **Aktivieren** wird der zu aktivierende Rechner in die Clientliste aufgenommen. Wenn alle zu schützenden Rechner aktiviert wurden, folgt nach einem Klick auf **Weiter** der nächste Schritt. Wenn Sie Clients aktiviert haben, ist das Häkchen bei **Client-Software automatisch auf den aktivierten Computern installieren** voreingestellt. Wenn die Verteilung der Software auf den Client-Rechnern zu einem späteren Zeitpunkt erfolgen soll, muss diese Option durch Entfernen des Häkchens deaktiviert werden.

Der G Data ManagementServer lädt über das Internet neue Virensignaturen und Programmdateien herunter. Damit dieser Vorgang automatisch erfolgen kann, ist die Eingabe der Zugangsdaten erforderlich, die bei der Online-Registrierung erstellt wurden. Es besteht auch die Möglichkeit, das Internet-Update nachträglich über die G Data Administrator-Programmoberfläche zu automatisieren. Eine detaillierte Beschreibung zur Planung von Updateintervallen finden Sie im Kapitel **Internet-Update**.

Klicken Sie auf **Weiter**, um die E-Mail-Benachrichtigungen zu konfigurieren. Im Fall eines Virenfundes auf einem oder mehreren Clients oder bei anderen kritischen Situationen kann der Netzwerkadministrator per Mail informiert werden. Wählen Sie dazu eine oder mehrere Empfängergruppe(n) aus oder klicken Sie auf das Zahnräder-Symbol, um das **E-Mail-Einstellungen**-Fenster zu öffnen. Über die **Begrenzung** lässt sich ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindern.

Um die Verwaltung mobiler Geräte zu ermöglichen, müssen einige grundlegende Einstellungen konfiguriert werden. Vergeben Sie dazu im nächsten Schritt ein Kennwort, mit dem sich mobile Geräte beim ManagementServer authentifizieren müssen. Um Notfallaktionen serverseitig über das Mobilgerät durchführen zu können, müssen Sie die **Sender-ID** und den **API-Key** von Ihrem Google Cloud Messaging-Konto eingeben. Kostenlose Konten für diese Push-Benachrichtigung können bei **code.google.com/apis/console** eingerichtet werden. Die Einstellungen können später durch Öffnen des **Mobile**-Karteireiters im Fenster **Server-Einstellungen** bearbeitet werden.

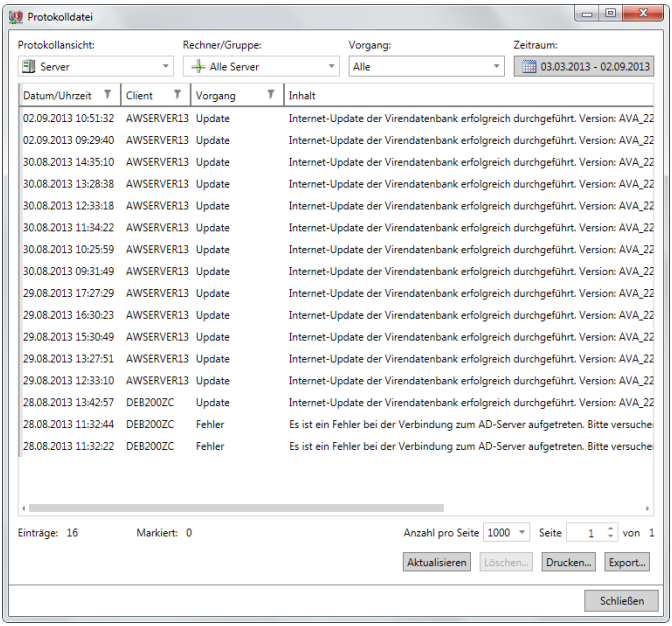
Mit **Fertigstellen** wird der Assistent beendet. Wenn Sie die Option **Client-Software automatisch auf den aktivierten Computern installieren** auswählen, führt der Einrichtungsassistent eine **Remote-Installation** des G Data Security Clients auf allen ausgewählten Netzwerk-Geräten durch.

4.2.1.2. Protokoll anzeigen

In der Protokolldatei steht ein Überblick über die letzten von der G Data Software durchgeführten Aktionen zur Verfügung. Hier werden sämtliche relevanten Informationen angezeigt. Die Anzeige des Protokolls kann nach folgenden Kriterien gefiltert werden:

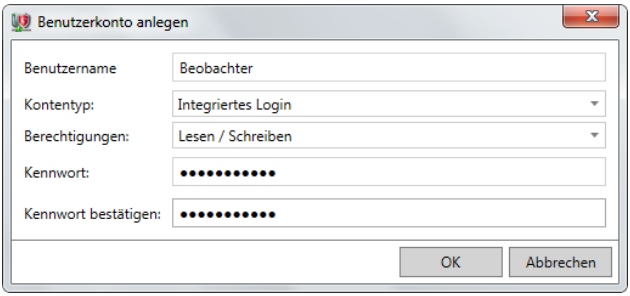
- **Protokollansicht**: Legen Sie hier fest, ob Sie ein Protokoll von den Client- oder Servervorgängen einsehen möchten.
- **Rechner/Gruppe**: Hier können Sie festlegen, ob Sie sich ein Protokoll aller Clients bzw. Gruppen oder nur einzelner Bereiche anschauen möchten.
- **Vorgang**: Definieren Sie hier, ob Sie alle protokollierten Informationen einsehen möchten oder nur Meldungen zu bestimmten Themen.
- **Zeitraum**: Hier können Sie den von/bis Zeitraum definieren, für den Protokollinformationen eingesehen werden sollen.

Das Feld **Aktualisieren** dient dazu, Vorgänge mit aufzulisten, die sich ereignen, während die Protokollansicht geöffnet ist. Sämtliche Vorgänge erscheinen erst einmal in chronologischer Reihenfolge und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach bestimmten Kriterien sortieren. Sie können Vorgänge exportieren, drucken oder löschen.


Protokolldatei
Protokollansicht:
Server
Rechner/Gruppe:
Alle Server
Vorgang:
Alle
Zeitraum:
03.03.2013 - 02.09.2013
Datum/Uhrzeit
Client
Vorgang
Inhalt
02.09.2013 10:51:32 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
02.09.2013 09:29:40 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 14:35:10 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 13:28:38 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 12:33:18 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 11:34:22 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 10:25:59 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
30.08.2013 09:31:49 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
29.08.2013 17:27:29 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
29.08.2013 16:30:23 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
29.08.2013 15:30:49 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
29.08.2013 13:27:51 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
29.08.2013 12:33:10 AWSERVER13 Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
28.08.2013 13:42:57 DEB200ZC Update Internet-Update der Virendatenbank erfolgreich durchgeführt. Version: AVA_22
28.08.2013 11:32:44 DEB200ZC Fehler Es ist ein Fehler bei der Verbindung zum AD-Server aufgetreten. Bitte versuche
28.08.2013 11:32:22 DEB200ZC Fehler Es ist ein Fehler bei der Verbindung zum AD-Server aufgetreten. Bitte versuche
Einträge: 16
Markiert: 0
Anzahl pro Seite 1000
Seite 1 von 1
Aktualisieren
Löschen...
Drucken...
Export...
Schließen

4.2.1.3. Benutzerverwaltung

Als Systemadministrator können Sie weitere Benutzerzugänge für das G Data Administrator-Interface vergeben. Klicken Sie dazu auf die **Neu**-Schaltfläche und geben anschließend den **Benutzernamen**, die **Berechtigungen** dieses Nutzers (**Lesen**, **Lesen/Schreiben**, **Lesen/Schreiben/Backups wiederherstellen**) ein, definieren Sie den **Kontentyp** (**Integriertes Login**, **Windows-Benutzer**, **Windows-Benutzergruppe**) und vergeben Sie ein **Kennwort** für diesen Benutzer.

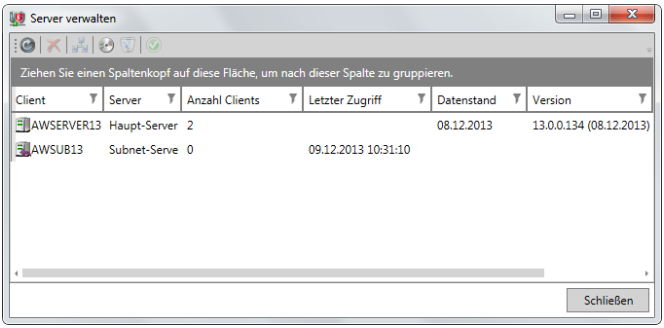


4.2.1.4. Serververwaltung

Über die Server-Verwaltung können Sie Clients einzelnen Subnet-Servern zuordnen, die dann die Kommunikation dieser Clients mit dem Main-Server bündeln und auf diese Weise die Netzwerknutzung optimieren. Die Zuordnung der Clients zu Subnet-Servern ist unabhängig von der Gruppierung von Clients im Clientauswahlbereich. Daher können Clients, die unterschiedlichen Subnet-Servern zugeordnet sind, dennoch in Gruppen unterteilt werden.

- **Löschen**: Entfernt einen oder mehrere Subnet-Server aus der Liste. Die eigentliche Software auf dem Subnet-Server wird nicht entfernt.
- **Clients zuordnen**: Über Clients zuordnen können Sie vorhandene Clients den definierten Subnet-Servern zuordnen.
- **Subnet-Server hinzufügen**: Klicken Sie auf Subnet-Server hinzufügen, um einen neuen Subnet-Server zu konfigurieren. Geben Sie den **Computernamen** des Subnet-Servers, sowie ein **Benutzerkonto** mit Administrator-Berechtigungen auf dem neuen Subnet-Server ein. Bestätigen Sie die Eingaben mit **OK**, um eine Remote-Installation zu starten. Das Fenster **Installationsübersicht** ermöglicht es Ihnen, den Installationstatus zu beobachten. Die Remote-Installation für Subnet-Server hat die gleichen Voraussetzungen wie eine **Client-Remote-Installation**.
- **Server deinstallieren**: Initialisiert eine Remote-Deinstallation der gewählten Subnet-Server.
- **Autorisation erteilen**: Um unberechtigten Zugriff auf Server-Daten zu verhindern, müssen lokal installierten Subnet-Server autorisiert werden. Erst nach der Autorisation wird der Managementserver Daten mit dem Subnet-Server synchronisieren.

  Nur lokal installierte Subnet-Server und Subnet-Servern, die auf Version 13 aktualisiert worden sind, müssen manuell autorisiert werden. Subnet-Server, die über eine Remote-Installation hinzugefügt worden sind, werden automatisch autorisiert. Eine Remote-Deinstallation kann nur für autorisierte Subnet-Server vorgenommen werden.



4.2.1.5. Subnet-Server-Synchronisation

Um eventuelle Änderungen auch außerhalb des regulären Kommunikationsintervalls von Server und Subnet-Server zu ermöglichen, kann die Subnet-Server-Synchronisation auch manuell angestoßen werden.

4.2.1.6. Beenden

Über diese Funktion wird der G Data Administrator geschlossen. Der G Data ManagementServer bleibt weiterhin gestartet und steuert den Virenschutz im Netzwerk gemäß der festgelegten Vorgaben.

4.2.2. Optionen

In der Menüleiste bietet das Menü Optionen Zugriff auf Einstellungen, die sich mit der Funktionalität des ManagementServer beschäftigen. Einige der Optionen werden automatisch konfiguriert, wenn Sie den **Server-Einrichtungsassistent** verwenden (z. B. **Internet-Update**), andere sollten manuell konfiguriert werden.

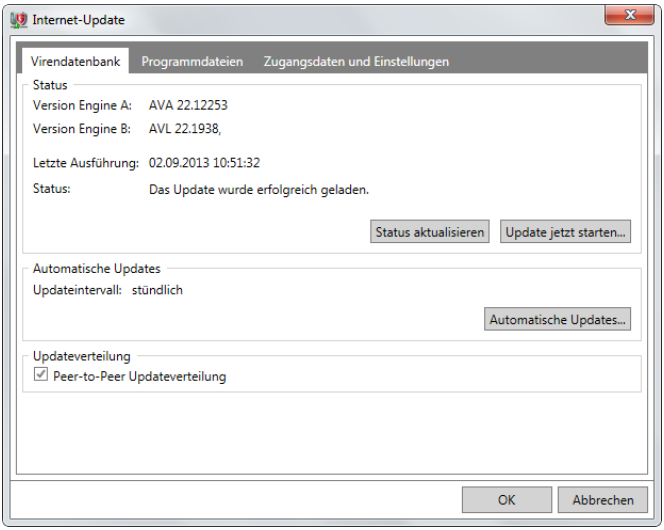
4.2.2.1. Internet-Update

Hier werden alle Einstellungen für Internet-Updates der Virendatenbanken und der Programmdateien der G Data Software festgelegt. In der Karteikarte **Zugangsdaten und Einstellungen** sind die Zugangsdaten einzugeben, die bei der Online-Registrierung erstellt wurden. Beim Internet-Update werden die aktuellen Virendefinitionen vom G Data UpdateServer geladen und auf dem G Data ManagementServer gespeichert. Die Nachfolgende Verteilung der Virensignaturen an die Clients wird vom Aufgabenbereich **Clients** gesteuert.

Virendatenbank

Alle Clients haben eine eigene, lokale Kopie der Virendatenbank, damit der Virenschutz auch gewährleistet ist, wenn sie offline sind (d.h. keine Verbindung mit dem G Data ManagementServer bzw. dem Internet besteht). Die Aktualisierung der Dateien auf den Clients erfolgt in zwei Schritten, die natürlich beide automatisiert werden können.

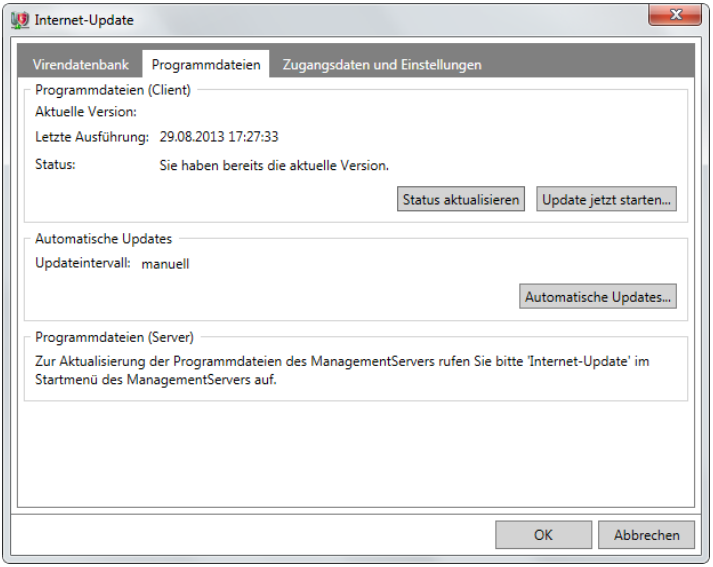
Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt (siehe Aufgabebereich **Client-Einstellungen** > **Allgemein**).



- **Status aktualisieren**: Über diese Schaltfläche können Sie die Statusanzeige der Virensignaturen gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten**: Über die Schaltfläche Update jetzt starten können Sie eine Aktualisierung der Virendatenbanken direkt durchführen. Dabei werden die aktuellen Virensignaturen heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.
- **Automatische Updates**: Wie die Virenprüfungen können Sie auch die Internet-Updates automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat. Damit das Update automatisch erfolgen kann, muss Ihr G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls Benutzerkonto und Proxy-Einstellungen vor.
- **Updateverteilung**: Die Verteilung kann zentral (MMS, SubnetServer > Clients) oder - wenn Sie das entsprechende Häkchenfeld aktivieren - auch dezentral (Peer to Peer) (MMS, SubnetServer, schon upgedatete Clients > Clients) erfolgen. Bitte achten Sie darauf, dass für die Updateverteilung ggf. die **Port-Konfiguration** angepasst werden muss.

Programmdateien

Wenn ein Programmupdate für die Client-Software von G Data bereit steht, können Sie die Aktualisierung der Clients über den G Data ManagementServer automatisch erledigen lassen. Die Aktualisierung der Dateien auf den Clients erfolgt in zwei Schritten, die beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt und damit wird der dortige Client aktualisiert (siehe Aufgabebereich **Client-Einstellungen** > **Allgemein**).

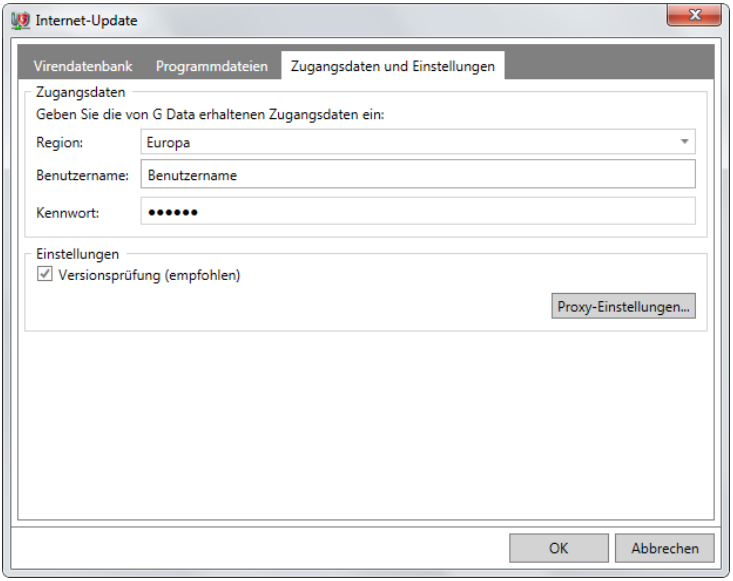


- **Status aktualisieren**: Über die Schaltfläche Aktualisieren können Sie die Statusanzeige der Softwareversion gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten**: Über die Schaltfläche Update jetzt starten können Sie eine Aktualisierung der Client-Software direkt durchführen. Dabei werden die aktuellen Clientdateien heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.
- **Automatische Updates**: Wie die Virenprüfungen können Sie auch die Internet-Updates der Client-Software automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat. Damit das Update automatisch erfolgen kann, muss der G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls Benutzerkonto und Proxy-Einstellungen vor.

Um die Programmdateien des G Data ManagementServers zu aktualisieren, rufen Sie in der Programmgruppe G Data ManagementServer im Startmenü den Eintrag Internet-Update auf. Der G Data ManagementServer kann ausschließlich über diesen Eintrag aktualisiert werden. Dagegen kann die G Data Client-Software auch über den G Data Administrator aktualisiert werden.

Zugangsdaten und Einstellungen

Mit der Online-Registrierung erhalten Sie von G Data die Zugangsdaten für das Update der Virendatenbanken und Programmdateien. Geben Sie diese unter **Benutzername** und **Kennwort** ein. Wählen Sie unter **Region** den nächsten Update-Server aus, um beim Herunterladen von Updates eine optimale Geschwindigkeit zu gewährleisten. Die standardmäßig aktivierte **Versionsprüfung** sollte im Regelfall immer eingeschaltet sein, da sie so die optimale Update-Geschwindigkeit gewährleistet. Sollten jedoch Probleme mit den lokalen Virendatenbankdateien auftreten, dann schalten Sie die Versionsprüfung aus. Auf diese Weise wird beim nächsten Internet-Update die Integrität aller Virendatenbankdateien überprüft und die fehlerhafte Dateien werden neu heruntergeladen.



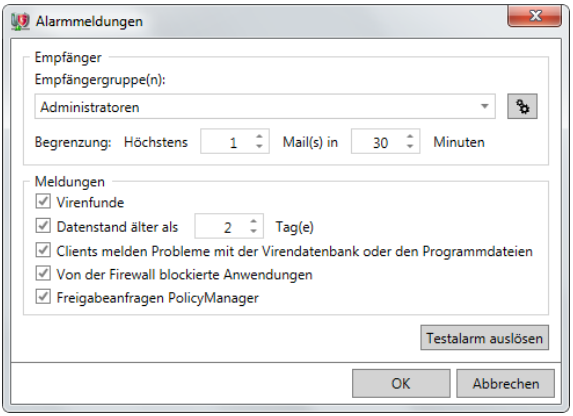
Mit der Schaltfläche **Proxy-Einstellungen** öffnen Sie ein Fenster, in dem Sie Zugangsdaten für Internet & Netzwerk eingeben können. Sie sollten hier nur Eingaben tätigen, wenn sich mit den Standardeinstellungen der G Data Software Probleme ergeben sollten (z.B. wegen der Verwendung eines Proxyservers) und ein Internet-Update nicht durchführbar ist.

Die G Data Software kann die Verbindungsdaten des Internet Explorer (ab Version 4) verwenden. Konfigurieren Sie zunächst den Internet Explorer und

prüfen Sie, ob die Testseite unseres Update-Servers erreichbar ist: http://ieupdate.gdata.de/test.htm. Schalten Sie anschließend die Option **Proxyserver verwenden** aus. Geben Sie unter **Benutzerkonto** das Konto ein, für den Sie den Internet Explorer konfiguriert haben (als das Konto, mit dem Sie sich an Ihrem Rechner angemeldet haben).

4.2.2.2. Alarmmeldungen

Bei neuen Virenfunden kann der G Data ManagementServer automatisch Alarmmeldungen per E-Mail versenden. Die dazu benötigten Einstellungen werden in diesem Bereich vorgenommen. Aktivieren Sie die E-Mail-Benachrichtigung, indem Sie das Häkchen bei den jeweils meldbaren Ereignissen setzen. Über die **Begrenzung** kann ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindert werden. Klicken Sie auf **Testalarm auslösen**, um der Empfängergruppe einen Testalarm zu schicken.



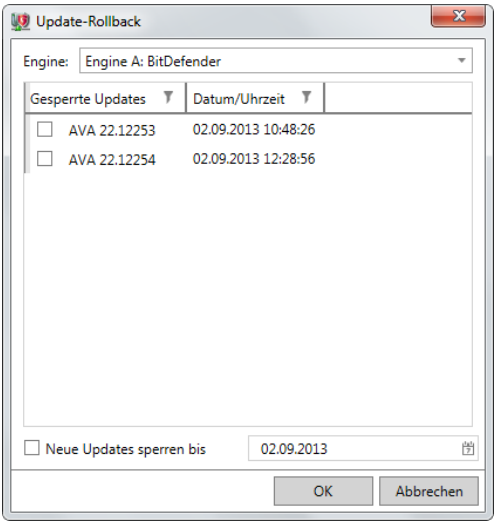
Um Änderungen an den **E-Mail-Einstellungen** vorzunehmen, klicken Sie bitte auf die Schaltfläche für erweiterte Einstellungen ( ).

4.2.2.3. Update-Rollback

Es kann im seltenen Fall von Fehlalarmen oder ähnlichen Problemen sinnvoll sein, das aktuelle Update der Virensignaturen zu sperren und stattdessen eines der vorhergehenden Signaturupdates zu verwenden. Der G Data ManagementServer speichert von jeder AntiViren-Engine die letzten Updates. Sollte es also mit dem aktuellen Update der Engine A oder B Probleme geben, kann der Netzwerkadministrator das aktuelle Update für einen bestimmten Zeitraum sperren und stattdessen automatisch das zeitlich davorliegende Signaturupdate an die Clients und Subnet-Server verteilen. Die Anzahl der zu speichernden Rollbacks können Sie im Bereich **Server-Einstellungen** vornehmen. Standardmäßig werden die letzten fünf Signaturstände gespeichert.

Auf Clients, die nicht mit dem G Data ManagementServer verbunden sind (z.B. Notebooks auf Dienstreisen) können keine Rollbacks durchgeführt werden. Eine vom Server an den Client übertragene Sperrung neuer Updates kann dort ohne Kontakt zum G Data ManagementSever nicht rückgängig gemacht werden.

Für die ausgewählte **Engine** werden hier die jüngsten Engine-Updates unter **Gesperrte Updates** aufgelistet. Wählen Sie das oder die Updates, die blockiert werden sollen, und klicken Sie auf OK. Diese Updates werden dann nicht mehr verteilt werden, und Clients, die sie vorher erhalten haben, werden wieder zurückgesetzt auf das jüngste nicht gesperrte Update. Dies geschieht, sobald diese sich mit dem ManagementServer verbinden. Optional können Sie automatisch neue Updates bis zu einem bestimmten auswählbaren Datum sperren. Erst dann werden die Updates auf den Clients eingespielt. Nutzen Sie hierzu die Funktion **Neue Updates sperren bis**.



4.2.2.4. Server-Einstellungen

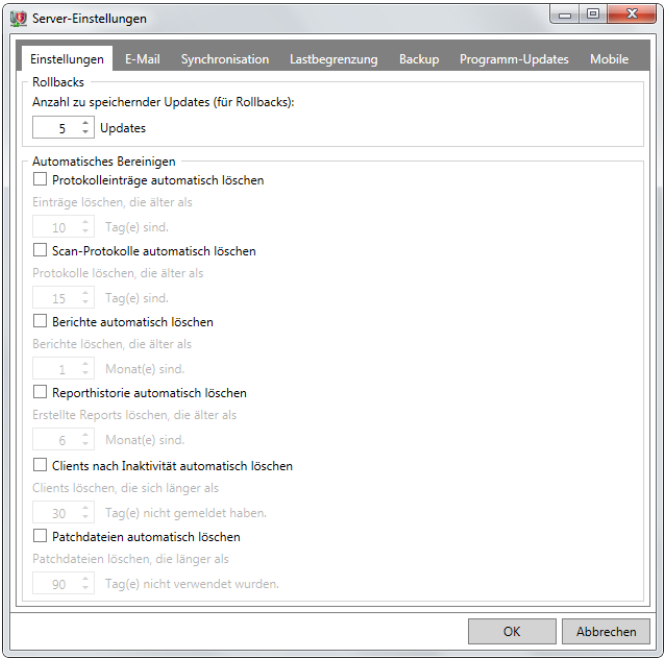
Das Server-Einstellungen-Fenster bündelt Konfigurationseinstellungen für ManagementServer-Funktionalitäten wie Synchronisation, E-Mail-Einstellungen, Lastbegrenzung und stufenweise Verteilung.

Einstellungen

Geben Sie unter **Rollbacks** an, wie viele der aktualisierten Virensignaturupdates Sie für Rollbacks als Reserve vorhalten möchten. Als Standardwert gelten hier jeweils die letzten fünf Signatur-Updates der jeweiligen Engine.

Legen Sie unter **Automatisches Bereinigen** fest, ob alte Updates automatisch nach einer gewissen Zeit gelöscht werden sollen:

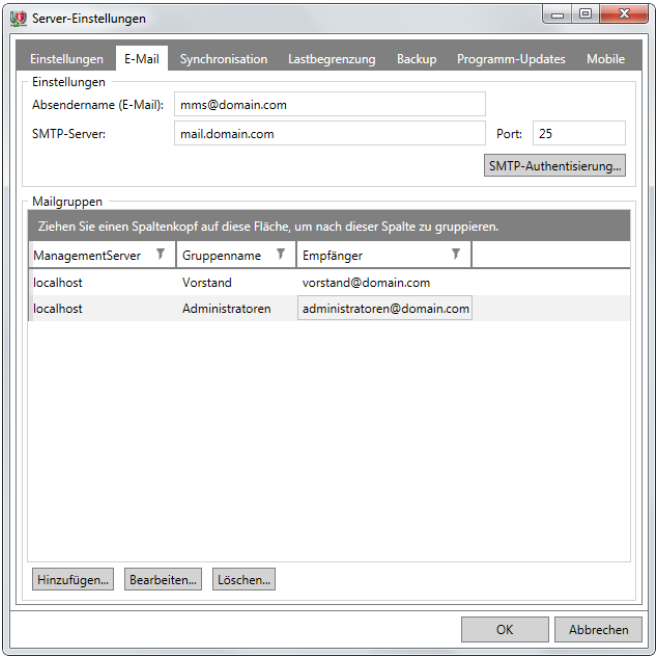
- **Protokolleinträge automatisch löschen**: Bestimmen Sie hier, dass Protokolleinträge nach einer gewissen Anzahl von Tagen gelöscht werden.
- **Scan-Protokolle automatisch löschen**: Löschen Sie hier Scan-Protokolle, die älter als eine gewisse Anzahl von Tagen sind.
- **Berichte automatisch löschen**: Legen Sie hier fest, dass Berichte nach einer gewissen Anzahl von Monaten gelöscht werden.
- **Reporthistorie automatisch löschen**: Hier können Sie die Reporthistorie nach einer gewissen Anzahl von Monaten löschen.
- **Clients nach Inaktivität automatisch löschen**: Löschen Sie hier Clients, wenn Sie eine gewisse Anzahl von Tagen nicht im Netzwerk eingeloggt waren.
- **Patchdateien automatisch löschen**: Hier können Sie Patchdateien automatisch nach einer vorgebbaren Zeit löschen.



E-Mail

Geben Sie hier den **SMTP-Server** und den **Port** (normalerweise 25) an, über den der G Data ManagementServer zum Versenden von Mails nutzen soll. Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die Mails verschickt werden können. An diese E-Mail-Adresse werden auch die Antworten der Internet-Ambulanz geschickt. Falls Ihr SMTP-Server Authentisierung erfordert, klicken Sie auf **SMTP-Authentisierung**. Sie können das Verfahren für **SMTP AUTH** konfigurieren (direkte Anmeldung am SMTP-Server) oder für **SMTP after POP3**.

Unter **Mailgruppen** können Sie Listen verschiedener Empfänger verwalten,,z.B. das Management-Team, Techniker usw.

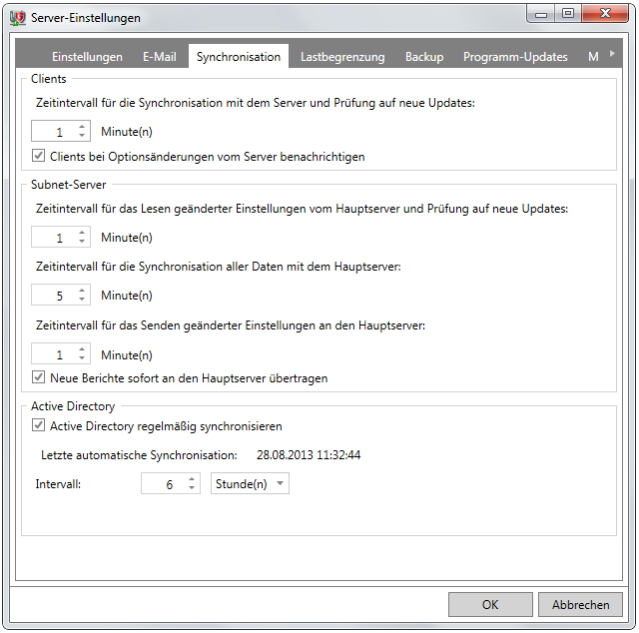


Synchronisation

Im Synchronisation-Bereich können Sie das Synchronisationsintervall zwischen Clients, Subnet-Servern und Servern definieren:

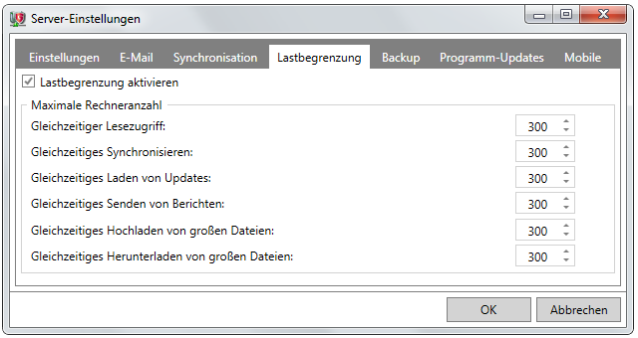
- **Clients**: Geben Sie hier das Zeitintervall an, in dem sich die Clients mit dem Server verbinden sollen, um zu prüfen, ob neue Updates und Einstellungen vorliegen. Als Standardwert sind fünf Minuten festgelegt. Wenn Sie das Häkchen bei **Clients bei Optionsänderungen vom Server benachrichtigen** setzen, werden die Client-Rechner direkt mit dem Server synchronisiert, unabhängig von vorgegebenen Synchronisationsintervallen.
- **Subnet-Server**: Über diesen Bereich können Sie die Intervalle für die Kommunikation zwischen Server und Subnet-Server definieren. Wenn Sie das Häkchen bei **Neue Berichte sofort an den Hauptserver übertragen** setzen, dann werden Berichte unabhängig von den hier vorgenommenen Einstellungen sofort an den Hauptserver übertragen.
- **Active Directory**: Legen Sie hier das Intervall fest, indem der G Data ManagementServer das Active Directory synchronisieren soll. Wenn Sie eine tägliche Synchronisation einstellen, können Sie die Active Directory-Synchronisation für einen bestimmten Zeitpunkt planen. Die Synchronisation des Active Directory erfolgt nur, wenn mindestens eine Gruppe einem Active

Directory-Eintrag **zugewiesen** wurde.



Lastbegrenzung

Wenn das Häkchen beim Eintrag **Lastbegrenzung aktivieren** gesetzt ist, lässt sich festlegen, wie viele Clients gleichzeitig die darunter aufgeführten Aktionen ausführen dürfen. So kann die Last verteilt werden, sodass es z.B. durch das gleichzeitige Laden von Updates zu keiner Latenzerhöhung im Netzwerk kommt.



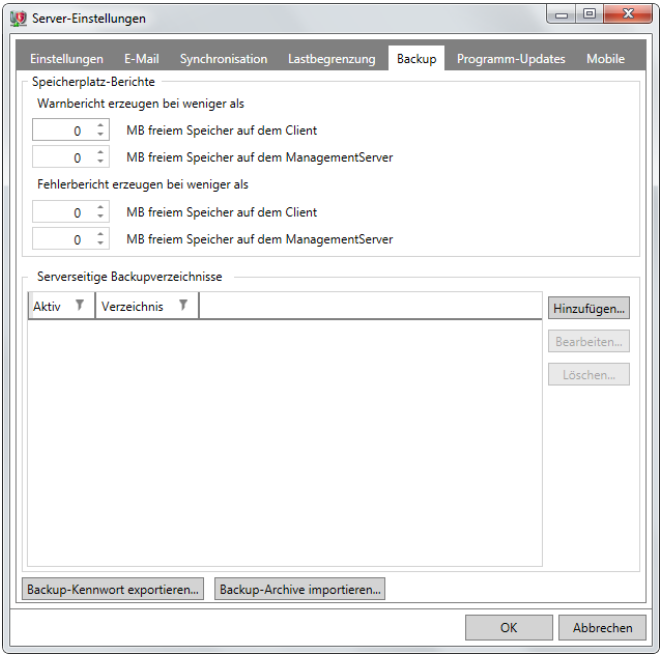
Backup

Um sicherzustellen, dass Backupaufträge erfolgreich ausgeführt werden können, sollte sowohl auf dem Server (Backup-Speicher), als auch auf dem Client (Backup-Cache) ausreichend Speicherplatz verfügbar sein. Wenn der Speicherplatz den Schwellenwert

für Warnberichte unterschreitet, wird unter **Berichte** ein Warnbericht erzeugt und den Client-Cache automatisch gereinigt. Alle Backup-Archive, außer das neueste, werden gelöscht (nur wenn sie schon zum ManagementServer hochgeladen worden sind). Wenn der Schwellenwert für Fehlerberichte unterschritten wird, erzeugt der ManagementServer einen Fehlerbericht. Der Backup-Speicher und der Client-Cache werden gereinigt. Falls danach immer noch nicht genügend Speicherplatz verfügbar ist, werden Backups nicht mehr durchgeführt.

Unter **Serverseitige Backupverzeichnisse** kann ein Pfad angegeben werden, auf dem alle auflaufenden Backups gespeichert werden sollen. Wird hier kein Verzeichnis angegeben, werden alle Backups unter C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup bzw. C:\Dokumente und Einstellungen\All Users \Anwendungsdaten\G DATA\AntiVirus ManagementServer\Backup gespeichert.

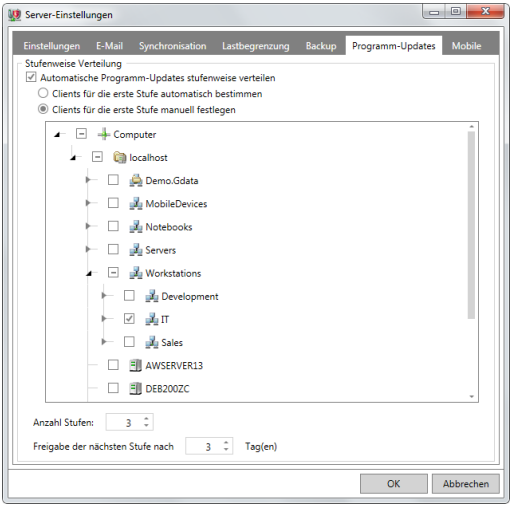
Da sämtliche mit der G Data Software erstellten Backups verschlüsselt sind, besteht auch die Möglichkeit, die Passwörter für die Backups zu exportieren und für eine spätere Verwendung zu speichern. Die Schaltfläche **Backup-Archive importieren** ermöglicht den Zugriff auf Backups, die in anderen Ordnern gespeichert sind.



Programm-Updates

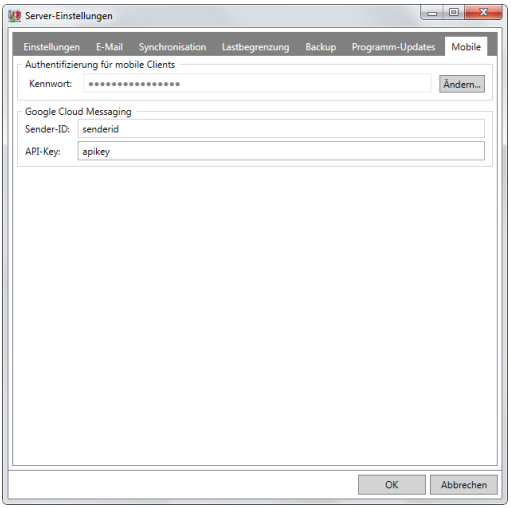
Im Bereich **Stufenweise Verteilung** können Sie festlegen, ob Sie Programmupdates zeitgleich auf allen Clients einspielen oder stufenweise. Eine stufenweise Verteilung verringert die Systemlast, die bei so einem Programmupdate unvermeidlich ist. Wenn Sie sich für eine stufenweise Verteilung entscheiden, können Sie festlegen, ob die

Verteilung automatisch erfolgt oder selber festlegen, welche Clients zuerst mit Programm-Updates versehen werden sollen, welche Clients danach kommen und wie weit die Untergliederung in verschiedene Verteilungsstufen untergliedert ist.



Mobile

Der Karteireiter Mobile verfügt über einige allgemeine Einstellungen zur Verwaltung mobiler Geräte. Soweit die Einstellungen nicht mithilfe des **Server-Einrichtungsassistenten** vorkonfiguriert wurden, können Sie hier die Authentifizierung für mobile Clients und das Google Cloud Messaging konfigurieren.

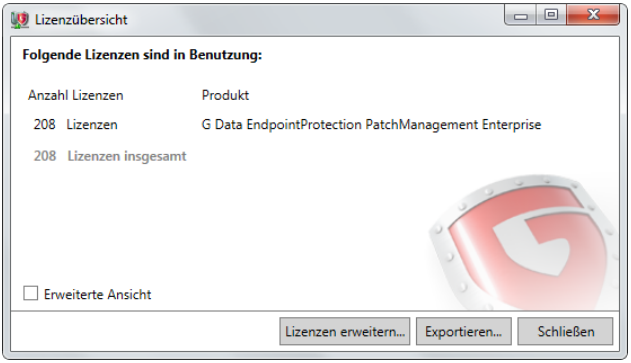


Geben Sie bitte unter **Authentifizierung für mobile Clients** ein **Kennwort** ein, mit dem sich das Mobilgerät beim ManagementServer authentifizieren kann. Um Notfallaktionen serverseitig über das Mobilgerät durchführen zu können, müssen Sie die **Sender-ID** und den **API-Key** von Ihrem Google Cloud Messaging-Konto eingeben. Kostenlose Konten für diese Push-Benachrichtigung können bei **code.google.com/apis/console** eingerichtet werden. Weitere Informationen hierzu finden Sie im Reference Guide.

4.2.3. Lizenz-Management

Über die Lizenzübersicht haben Sie jederzeit Überblick darüber, wie viele Lizenzen Ihrer G Data Software in Ihrem Netzwerk installiert sind. Wenn Sie weitere Lizenzen benötigen, können Sie direkt über die Schaltfläche **Lizenzen erweitern** mit dem G Data Upgrade-Center Kontakt aufnehmen.

Über die Schaltfläche **Exportieren** haben Sie die Möglichkeit, sich eine Übersicht Ihrer verwendeten Lizenzen als Textdatei ausgeben zu lassen. Wenn Sie hier das Häkchen bei **Erweiterte Ansicht** setzen, erhalten Sie die Information darüber, auf welchem Server explizit welche Lizenzen eingesetzt werden.

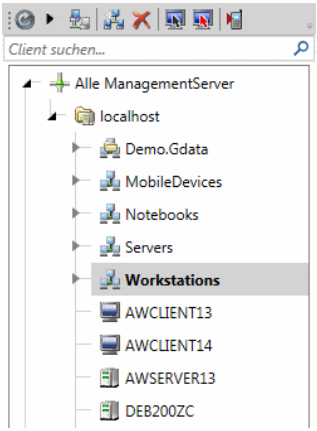


4.3. Clientauswahlbereich

Bevor Clients mithilfe des G Data Administrator verwaltet werden können, müssen diese im Client-Management-Bereich hinzugefügt und aktiviert werden. Es gibt mehrere Möglichkeiten zum Hinzufügen, abhängig von der Größe und Konfiguration des Netzwerks. Bei kleineren Netzwerken reicht es, Clients über den **Server-Einrichtungsassistenten** hinzuzufügen. Bei größeren Netzwerken kann das Verfahren über das **Computer suchen**-Dialogfenster oder über die integrierten **Active Directory-Unterstützung** gestrafft und (teilweise) automatisiert werden.

Hier werden sämtliche Clients und Server sowie definierte Gruppen in Ihrem Netzwerk aufgelistet. Wie im Windows Explorer erscheinen Gruppen, in denen sich Untergliederungen befinden, mit einem kleinen Plus-Symbol. Wenn Sie dieses anklicken, öffnet sich die Verzeichnisstruktur an dieser Stelle und ermöglicht die

Ansicht der darunter befindlichen Struktur. Ein Klick auf das Minus-Symbol schließt diese Untergliederung wieder. Zum Beispiel können Sie für PCs den Eintrag **Client-Einstellungen** aufrufen, um Ihre Optionen anzupassen. Bei mobilen Clients können Sie hingegen die **Mobile-Einstellungen** aufrufen.



Im Clientauswahlbereich können Sie bequem Einstellungen importieren und exportieren. Klicken Sie mit der rechten Maustaste auf einen Client und wählen Sie **Einstellungen exportieren**, um die Client- und PolicyManager-Einstellungen in einer .dbdat-Datei zu speichern. Um Einstellungen zu importieren, klicken Sie mit der rechten Maustaste auf einen Client oder eine Gruppe, wählen Sie **Einstellungen importieren** und selektieren Sie die gewünschten Einstellungsgruppen und die .dbdat-Datei.

Verschiedene Client-Typen werden durch unterschiedliche Symbole, wie z.B. für den ManagementServer, eine Gruppe, eine Active Directory-Gruppe, einen Desktop-Client oder einen mobilen Client angezeigt. Folgende Symbole sind in der Verzeichnisauswahl sichtbar:

- Netzwerk
- Server
- Subnet-Server
- Gruppe
- Gruppe (Active Directory)
- Client
- Linux-Client
- Laptop-Client
- Mobile-Client

Linux-Server

Nicht auswählbare Geräte: Hierunter fallen z.B. Netzwerkdrucker

In der Symbolleiste sehen Sie die wichtigsten Client-Management-Befehle, von denen einige auch in der **Organisation**-Menü angezeigt werden:

Aktualisieren

Alle erweitern/reduzieren: Hiermit können Sie die Ansicht Ihres Netzwerksverzeichnisses beeinflussen.

Deaktivierte Clients anzeigen

Neue Gruppe anlegen

Löschen

Client aktivieren: Zum Aktivieren eines Computers, markieren Sie ihn in der Liste und wählen dann die abgebildete Schaltfläche.

Installationsübersicht

Installationslink an mobile Clients senden: Um mobile Clients über den G Data Administrator zu verwalten, können Sie diesen einen Installationslink für die G Data Internet Security App per Mail schicken. Hierüber starten Sie dann die **Installation der G Data Internet Security für Android**.

4.3.1. Active Directory

Über die Active Directory-Integration können alle Computerobjekte der Organisationseinheiten der Domäne importiert werden. Dazu muss eine eigene Gruppe im G Data Administrator angelegt werden. Nach einem Rechtsklick auf die neu erstellte Gruppe wird der Menüpunkt **Active Directory Eintrag der Gruppe zuordnen** sichtbar. Im Dialogfenster, das sich öffnet, wählen Sie den Punkt **Einer Gruppe im Active Directory zuweisen** aus und geben den LDAP-Server an. Die **Auswahl**-Schaltfläche stellt eine Auswahl verfügbarer Server zur Verfügung. Auch das Verbinden mit einer anderen Domäne ist möglich. Die Option **G Data Security Client automatisch auf neu hinzugefügten Rechnern installieren** bewirkt dass auf jedem Rechner, der zur Active Directory-Domäne zugefügt wird, sofort der Client installiert wird, sofern er die Mindestvoraussetzungen erfüllt. Geben Sie dazu einen Domäne-**Benutzernamen** ein, der über ausreichende Berechtigungen auf den Clients verfügt, sowie das dazugehörende **Kennwort** und die Installations-**Sprache**.

Standardmäßig vergleicht der G Data ManagementServer seine Daten mit dem Active Directory alle sechs Stunden. Dieser Wert kann unter **Server-Einstellungen** > **Synchronisation** geändert werden.

4.3.2. Organisation

Clients können über den **Clientauswahlbereich** auf der linken Seite der Programmoberfläche verwaltet werden. Erweiterte Optionen können Sie im Organisation-Menü durchführen.

4.3.2.1. Aktualisieren

Um Änderungen im Netzwerk zu verfolgen, die sich zu der Zeit ergeben, in der Sie den G Data Administrator nutzen, können Sie die Aktualisieren-Funktion verwenden.

4.3.2.2. Deaktivierte Clients anzeigen

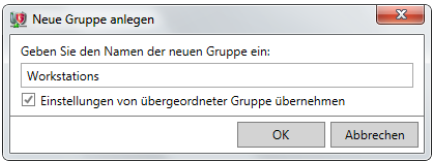
Clients, die nicht aktiviert sind, können über diese Funktion sichtbar gemacht werden. Deaktivierte Clients werden dabei als durchscheinende Symbole dargestellt. Aktivierte Clients sind durch vollfarbige Symbole gekennzeichnet.

Client (aktiviert)

Client (deaktiviert)

4.3.2.3. Neue Gruppe anlegen

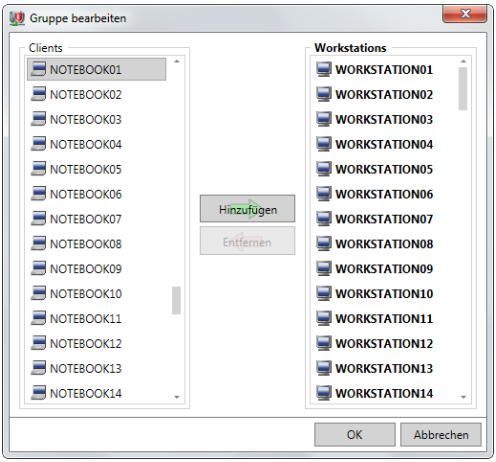
Über diesen Befehl lässt sich eine Gruppe anlegen. Damit lassen sich leicht unterschiedliche Sicherheitszonen definieren, da alle Einstellungen sowohl für einzelne Clients als auch für komplette Gruppen durchgeführt werden können. Nach dem Anwählen dieser Option und der Vergabe eines Gruppennamens können Clients der neuen Gruppe zugeordnet werden, indem man in der Clientliste den gewünschten Client mit der Maus, per Drag&Drop, auf die entsprechende Gruppe zieht.



Um eine große Anzahl von Clients in einer Gruppe zu bewegen, verwenden Sie den Modul **Clients** > **Übersicht**. Wählen Sie die Clients, die verschoben werden sollen, drücken Sie die rechte Maustaste und wählen Sie **G Data Security Client in Gruppe verschieben**.

4.3.2.4. Gruppe bearbeiten

Diese Option öffnet eine Dialogbox, in der sich über die Tasten **Hinzufügen** und **Entfernen** Clients zur Gruppe hinzufügen oder aus der Gruppe entfernen lassen. Nur verfügbar, wenn im Clientauswahlbereich eine Gruppe angewählt ist.



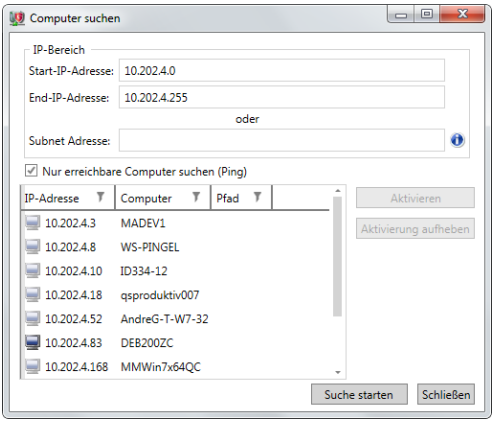
4.3.2.5. Löschen

Einzelne Clients lassen sich mit dem Befehl Löschen aus der Clientliste entfernen. Durch das Entfernen des Clients aus der Liste wird der G Data Security Client nicht deinstalliert.

> Um eine Gruppe zu löschen, müssen alle in ihr enthaltenen Clients nach Bedarf entweder deaktiviert oder in andere Gruppen verschoben werden. Nur leere Gruppen können gelöscht werden.

4.3.2.6. Computer suchen

Das Computer suchen-Fenster kann verwendet werden, um Netzwerk-Clients im G Data Administrator-Client-Management-Bereich hinzufügen und zu aktivieren. Clients können direkt aus dem Dialogfenster heraus über die IP-Adresse gefunden und aktiviert werden.



Über das Computer suchen-Fenster können alle alle Computer in einem bestimmten IP-Bereich kontaktiert werden. Der Bereich kann über eine **Start-IP-Adresse** und **End-IP-Adresse** (z.B. 192.168.0.1 und 192.168.0.255) oder die **Subnet-Adresse** (CIDR-Notation, z.B. 192.168.0.0/24) definiert werden. Um sicherzustellen, dass nur verfügbare Clients aufgelistet werden, wählen Sie die Option **Nur erreichbare Computer suchen (Ping)**. Klicken Sie auf **Suche starten**, um die Suche im Netzwerk zu beginnen. Computer werden nun aufgelistet, sobald sie gefunden werden. Wenn der Suchvorgang zu lange dauert, können Sie die Suche abbrechen durch Anklicken von **Suche abbrechen**.

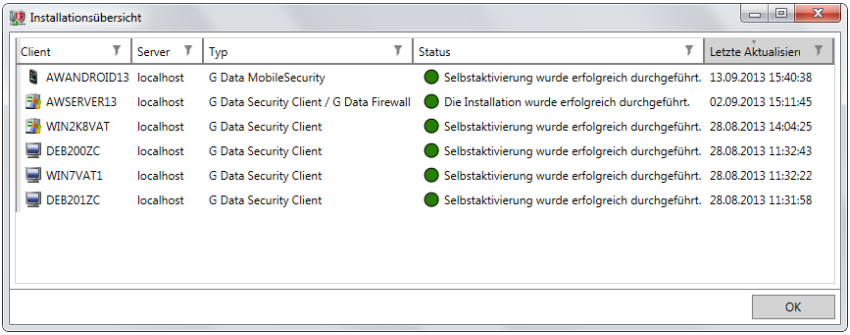
Alle Computer, die auf den IP-Check antworten, werden nun aufgelistet, einschließlich ihrer IP-Adresse und dem Namen des Computers. Mit der Schaltfläche **Aktivieren** können die jeweiligen Clients dem Clientauswahlbereich hinzugefügt werden. Im Suchergebnis können aktivierte Clients durch Anklicken von **Aktivierung aufheben** auch deaktiviert werden.

4.3.2.7. G Data Security Client Installationspaket erstellen

Über diese Funktion ist es möglich, ein Installationspaket für den G Data Security Client zu erstellen. Mit diesem Installationspaket können Sie den G Data Security Client lokal ohne Benutzerinteraktion einfach im Hintergrund installieren. Lesen Sie das Kapitel **Lokale Installation** für weitere Informationen.

4.3.3. Installationsübersicht

Um einen Überblick über den Installationsfortschritt zu erhalten, können Sie das Installationsübersichts-Fenster verwenden. Es wird automatisch geöffnet wenn ein Remote-Installationsauftrag hinzugefügt wird, aber es kann auch über die Installationsübersicht-Schaltfläche im Clientauswahlbereich geöffnet werden.

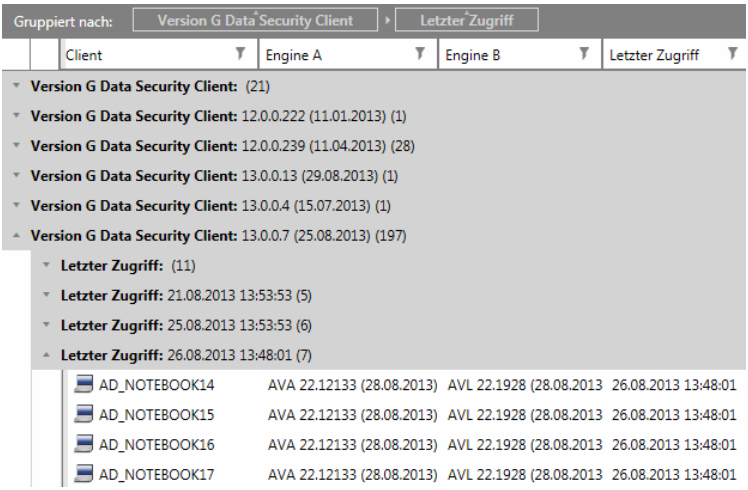

Installationsübersicht
Client
Server
Typ
Status
Letzte Aktualisieru
AWANDROID13 localhost G Data MobileSecurity Selbstaktivierung wurde erfolgreich durchgeführt. 13.09.2013 15:40:38
AWSERVER13 localhost G Data Security Client / G Data Firewall Die Installation wurde erfolgreich durchgeführt. 02.09.2013 15:11:45
WIN2K8VAT localhost G Data Security Client Selbstaktivierung wurde erfolgreich durchgeführt. 28.08.2013 14:04:25
DEB200ZC localhost G Data Security Client Selbstaktivierung wurde erfolgreich durchgeführt. 28.08.2013 11:32:43
WIN7VAT1 localhost G Data Security Client Selbstaktivierung wurde erfolgreich durchgeführt. 28.08.2013 11:32:22
DEB201ZC localhost G Data Security Client Selbstaktivierung wurde erfolgreich durchgeführt. 28.08.2013 11:31:58
OK

Die Installationsübersicht zeigt alle erledigten und unerledigten Remote-Installationsaufträge an. Die Spalte **Typ** zeigt den Typ der Installation (G Data Security Client und/oder G Data Firewall oder Subnet-Server). Sobald die Remote-Installation abgeschlossen ist, wird die **Status**-Spalte aktualisiert. In den meisten Fällen muss der Client neu gestartet werden um die Installation abzuschließen. Der Installationsvorgang

erzeugt einen entsprechenden **Bericht**, wenn ein Neustart erforderlich ist.

4.4. Aufgabenbereiche

In den verschiedenen Aufgabenbereichen, die über die jeweiligen Karteireiter anwählbar sind, besteht die Möglichkeit, die Absicherung des gesamten Unternehmensnetzwerks und seiner Clients zu administrieren. Die Einstellungen, die dabei vorgenommen werden, beziehen sich immer auf die Clients oder Gruppen, die im Clientauswahlbereich markiert wurden. Die einzelnen Themenfelder werden in den folgenden Abschnitten eingehend erläutert.


Gruppiert nach:
Version G Data Security Client
Letzter Zugriff
Client
Engine A
Engine B
Letzter Zugriff
Version G Data Security Client: (21)
Version G Data Security Client: 12.0.0.222 (11.01.2013) (1)
Version G Data Security Client: 12.0.0.239 (11.04.2013) (28)
Version G Data Security Client: 13.0.0.13 (29.08.2013) (1)
Version G Data Security Client: 13.0.0.4 (15.07.2013) (1)
Version G Data Security Client: 13.0.0.7 (25.08.2013) (197)
Letzter Zugriff: (11)
Letzter Zugriff: 21.08.2013 13:53:53 (5)
Letzter Zugriff: 25.08.2013 13:53:53 (6)
Letzter Zugriff: 26.08.2013 13:48:01 (7)
AD_NOTEBOOK14 AVA 22.12133 (28.08.2013) AVL 22.1928 (28.08.2013 26.08.2013 13:48:01
AD_NOTEBOOK15 AVA 22.12133 (28.08.2013) AVL 22.1928 (28.08.2013 26.08.2013 13:48:01
AD_NOTEBOOK16 AVA 22.12133 (28.08.2013) AVL 22.1928 (28.08.2013 26.08.2013 13:48:01
AD_NOTEBOOK17 AVA 22.12133 (28.08.2013) AVL 22.1928 (28.08.2013 26.08.2013 13:48:01

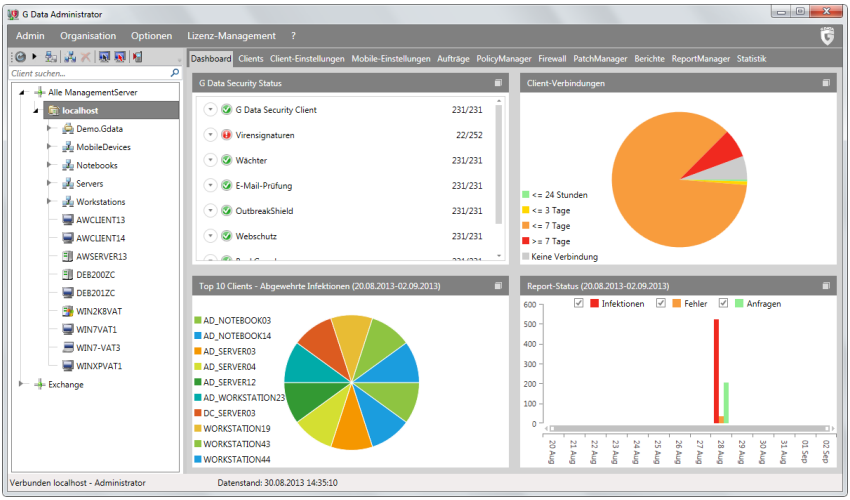
Für die meisten Module gibt es allgemeine Optionen, um das Layout und den Inhalt der Listen im Infobereich zu editieren. Zum Beispiel kann die Anzahl der **Einträge pro Seite** reduziert werden. Wählen Sie hierzu die maximale Anzahl pro Seite am unteren rechten Rand der Programmoberfläche aus. Für die Eingabe von Freitext-Filtern klicken Sie auf eine der Filter-Schaltflächen in den Spaltenüberschriften und geben Sie dort Ihre Filterkriterien ein. Neben dem Filter können Sie Listenelemente auch durch die Verwendung von Gruppen sortieren. Ziehen Sie dazu eine oder mehrere Spaltenüberschriften auf die Leiste oberhalb der Spaltenüberschriften, um eine Gruppe aus dieser Spalte zu erstellen. Gruppen können in unterschiedlicher Weise und in unterschiedlichen Ansichten erzeugt und verschachtelt werden.

Geänderte Einstellungen werden erst nach Betätigung der **Übernehmen**-Schaltfläche gespeichert. Drücken Sie die **Verwerfen**-Schaltfläche, um die aktuellen Einstellungen vom ManagementServer zu laden, ohne die Änderungen zu übernehmen. Sollten Clients innerhalb einer Gruppe unterschiedliche Einstellungen haben, bekommen einzelne Parameter, die unterschiedlich eingestellt sind, einen undefinierten Status. Die Clients der Gruppe haben in diesem Fall unterschiedliche Einstellungen für die Parameter. Undefinierte Parameter werden beim Übernehmen nicht gespeichert. In den meisten Modulen wird Ihnen unter **Information** angezeigt, ob die durchgeführten

Änderungen schon für den Client oder die Gruppe übernommen wurden.

4.4.1. Dashboard

Im Dashboard-Bereich erhalten Sie Informationen zum aktuellen Zustand der Clients im Netzwerk. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.



Unter **G Data Security Status** können Sie alle grundlegenden Sicherheitseinstellungen für die Clients oder Gruppen einstellen, die Sie im Clientauswahlbereich markiert haben.

Solange das Netzwerk optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Symbol.

Sollte mindestens eine Komponente nicht optimal eingestellt sein (z.B. abgeschalteter Wächter oder veraltete Virensignaturen), weist ein Achtung-Symbol darauf hin.

Wenn sich die G Data-Programmoberfläche öffnet, sind in einigen Fällen für kurze Zeit die meisten Symbole im Info-Modus. Das heißt nicht, dass das Netzwerk in diesem Moment ungeschützt ist. In diesem Moment wird die Datenbank des G Data ManagementServers vom G Data Administrator abgefragt.

Durch Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Aufgabenbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Symbol.

Der Bereich **Client-Verbindungen** bietet eine zeitliche Übersicht über die Verbindungen, die die jeweiligen Clients mit dem G Data ManagementServer hatten. Es sollte darauf geachtet werden, dass sich alle Clients regelmäßig mit dem G Data ManagementServer verbinden. Die Clients die z.B. aufgrund des Nutzerverhaltens oder technischer Umstände in die Liste **Top 10 Clients - Abgewehrte Infektionen** erscheinen, sollten besonders beobachtet werden. Ein Auftauchen eines oder mehrerer Clients in diesem Bereich ist unter Umständen eine Indikation dafür, dass der Client-Anwender auf eventuelle Probleme aufmerksam gemacht werden oder technische Maßnahmen ergriffen werden sollten. Wenn die Infektionen auf Grund des Nutzerverhaltens stattfinden, wäre z.B. eine Nutzung des **PolicyManagers** (verfügbar in der Programmversion G Data EndpointProtection) ratsam. Der **Report-Status** bietet eine übersichtliche Darstellung über die Menge der Infektionen, Anfragen und Fehler in Ihrem Netzwerk innerhalb der letzten 30 Tage.

4.4.2. Clients

Unter Clients lässt sich überprüfen, ob die Clients ordnungsgemäß laufen und ob die Virensignaturen und Programmdateien auf dem neuesten Stand sind.

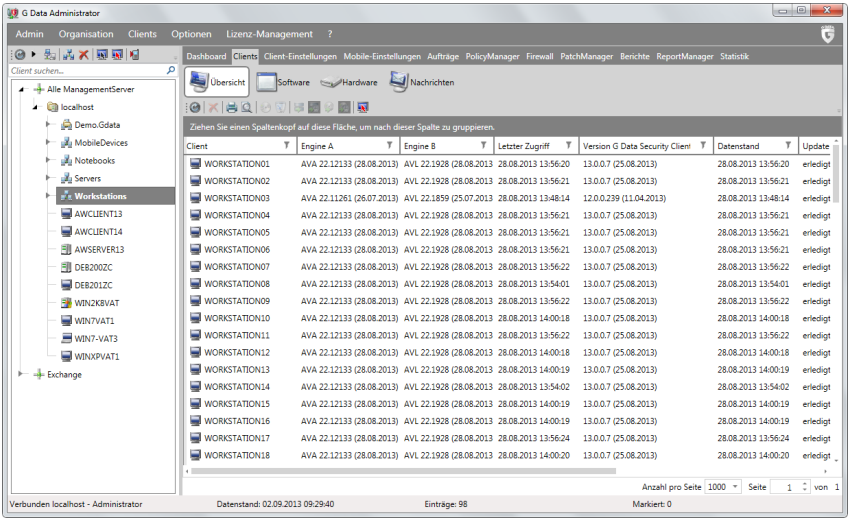
4.4.2.1. Übersicht

Hier erhalten Sie eine Übersicht über alle verwalteten Clients und können diese gleichzeitig auch administrieren. Mit Hilfe der Spalte **Security-Status** behalten Sie den Sicherheitsstatus jedes Clients im Blick.

Mit einem rechten Mausklick auf die Spaltenüberschriften können Sie weiterführende Informationsspalten zum Client zu- oder abwählen:

- **Server**
- **Alias (server)**
- **Client**
- **Security-Status**
- **Engine A**
- **Engine B**
- **Datenstand**
- **Version G Data Security Client**
- **Sprache**
- **UPMS-Client**
- **Letzter Zugriff**
- **Update Virendatenbank / Zeitpunkt**
- **Update Programmdateien / Zeitpunkt**
- **Betriebssystem**

- **Subnet-Server**
- **Domain**
- **Netzwerkkarte**
- **MAC-Adresse**
- **IPv4-Adresse**
- **IPv6-Adresse**
- **Subnetz-Maske**
- **Standardgateway**
- **DNS-Server**
- **DHCP-Server**
- **Primary WINS**
- **Secondary WINS**
- **Eula**



Zur Administration der Clients und Gruppen stehen Ihnen folgende Schaltflächen zur Verfügung:

Aktualisieren

Löschen: Hiermit entfernen Sie einen Client aus der Clientübersicht. Da diese Funktion die Client-Software nicht vom Client entfernt, sollte sie nur für Clients, die bereits außer Betrieb genommen oder vom Netzwerk entfernt worden sind, benutzt werden. Wenn ein aktiver Client aus Versehen gelöscht wurde, wird er bei der nächsten ManagementServer-Synchronisation wieder zur Liste hinzugefügt (jedoch ohne spezifische Gruppeneinstellungen).

Drucken: Hiermit starten Sie den Druckvorgang für die Client-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Clients Sie ausdrucken möchten.

Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.

G Data Security Client installieren

G Data Security Client deinstallieren

Virendatenbank jetzt aktualisieren: Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom G Data ManagementServer.

Virendatenbank automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem G Data ManagementServer vorhanden sind und führen die Aktualisierung automatisch durch.

Programmdateien jetzt aktualisieren: Aktualisiert die Programmdateien auf dem Client. Es werden die Client-Programmdateien verwendet, die der G Data ManagementServer bereit hält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss.

Programmdateien automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Programmdateien. Die Clients prüfen periodisch, ob eine neue Version auf dem G Data ManagementServer existiert und führen die Aktualisierung automatisch durch.

Installationsübersicht

Wenn Sie die Option Übersicht ausgewählt haben, erscheint hier ein zusätzlicher Menü-Eintrag namens Clients. Hier finden Sie die Funktionen wieder, die Sie auch durch Anklicken eines oder mehrerer Clients mit der rechten Maustaste im Kontextmenü erhalten würden. Folgende Optionen stehen hier zur Verfügung:

- **G Data Security Client installieren**
- **G Data Security Client für Linux installieren**
- **G Data Security Client deinstallieren**
- **Installationsübersicht**
- **Auf Gruppeneinstellungen zurücksetzen**: Hiermit führen Sie ein Reset der Sicherheitseinstellungen für einen modifizierten Client auf die vorgegebenen Gruppeneinstellungen durch.
- **G Data Security Client in Gruppe verschieben**: Diese Funktion ermöglicht es Ihnen, ausgewählte Clients in eine existierende Gruppe zu verschieben. Wenn Sie diese Option auswählen, werden alle existierenden Gruppen in einem neuen Fenster angezeigt. Um nun den Client in eine Gruppe zu verschieben, wählen Sie die in Frage kommende Gruppe aus und klicken Sie auf **OK**.

- **Zugewiesene Eula ändern**: Weist eine zuvor definierte Eula dem ausgewählten Client zu (nur für mobile Clients).
- **Zugewiesene Eula löschen**: Entfernt eine zugewiesene Eula von den ausgewählten Clients (nur für mobile Clients).
- **Eulaverwaltung**
- **G Data Server zuordnen**: Wenn Sie die Möglichkeit haben, Clients speziellen Subnet-Servern über die Funktion **Server verwalten** zuzuweisen, haben Sie auch die Option diesen Vorgang über das Kontextmenü durchzuführen.
- **Virendatenbank jetzt aktualisieren**
- **Virendatenbank automatisch aktualisieren**
- **Programmdateien jetzt aktualisieren**
- **Programmdateien automatisch aktualisieren**
- **Neustart nach Aktualisierung der Programmdateien**: Legen Sie hier fest, wie der Client reagieren soll, nachdem die Programmdateien aktualisiert wurden. Wählen Sie die Option **Hinweisfenster auf dem Client anzeigen**, um den Anwender darüber zu informieren, dass er bei nächster Gelegenheit seinen Rechner neu starten sollte, damit das Programm-Update durchgeführt werden kann. Über **Bericht erzeugen** erhalten Sie im **Berichte**-Bereich Infos darüber, welche Clients aktualisiert wurden. Mit der Option **Neustart ohne Abfrage durchführen** können Sie das Update automatisch auf den Clients einspielen und diese zu einem Neustart zwingen.

G Data Security Client installieren

Wählen Sie die Option G Data Security Client installieren, um die **Remote-Installation** des G Data Security Clients auf allen ausgewählten Rechnern durchzuführen.

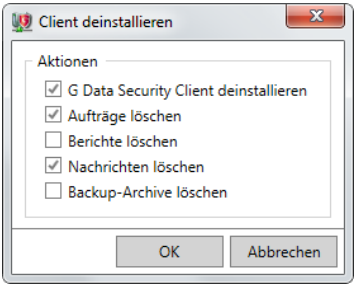
> Um auf deaktivierte Clients zugreifen zu können, müssen diese in der Clientübersicht als aktiv angezeigt werden. Bei Verwendung der Funktion G Data Security Client installieren weist Sie das Programm gegebenenfalls darauf hin und ermöglicht eine Darstellung der deaktivierten Clients.

Sollte die Software nicht über die Remote-Installation auf den Clients aufgespielt werden können, können Sie direkt am Clientrechner eine **lokale Installation** mit dem G Data-Installationsmedium oder einem Client-Installationspaket durchführen.

G Data Security Client deinstallieren

Diese Funktion erteilt dem G Data Security Client den Auftrag, sich selbst zu deinstallieren. Bevor die Deinstallation gestartet wird, können Sie die Komponenten auswählen, die behalten werden sollen. Es ist möglich, die Client-Software zu deinstallieren, während die Aufträge, Berichte, Nachrichten oder Backup-Archive, die diesem Client zugeordnet sind, weiterhin auf dem Server gespeichert bleiben. Wählen Sie die zu entfernenden Komponenten aus und klicken Sie auf **OK**, um die Deinstallation zu starten. Zum vollständigen Entfernen muss der Client neu gestartet

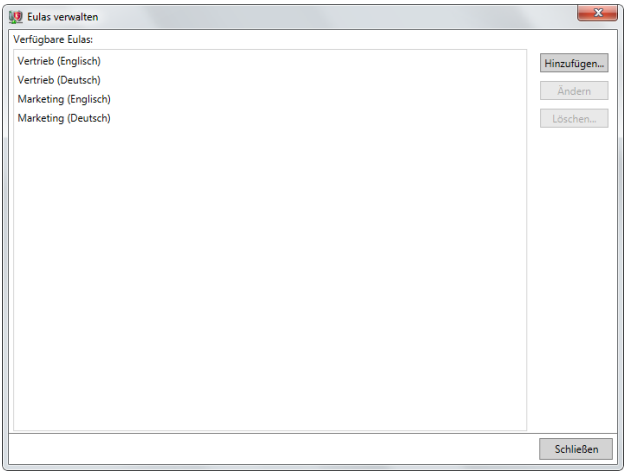
werden.



Alternativ ist es auch möglich, den Client lokal zu deinstallieren. Hierzu ist eine Eingabeaufforderung mit Administratorberechtigungen erforderlich. Wird im Verzeichnis C:\Programme (x86)\G DATA\AVKClient der Befehl *unclient /AVKUninst* abgesetzt, startet die Deinstallation. Gegebenenfalls wird ein Neustart verlangt. Sollte eine solche Anfrage nicht erscheinen, muss der Rechner nach max. 10 Minuten neu gestartet werden.

Eulas verwalten

Im Eulas verwalten-Fenster können Sie End User License Agreements (Eula) für mobile Geräte hinzufügen, bearbeiten und entfernen. Über die entsprechende Option im Clients-Menü kann die jeweilige Eula dann auf jedem mobilen Gerät zugewiesen werden, um sicherzustellen, dass die Endnutzer informiert und mit dem Einsatz der G Data Internet Security-Lösung einverstanden sind.

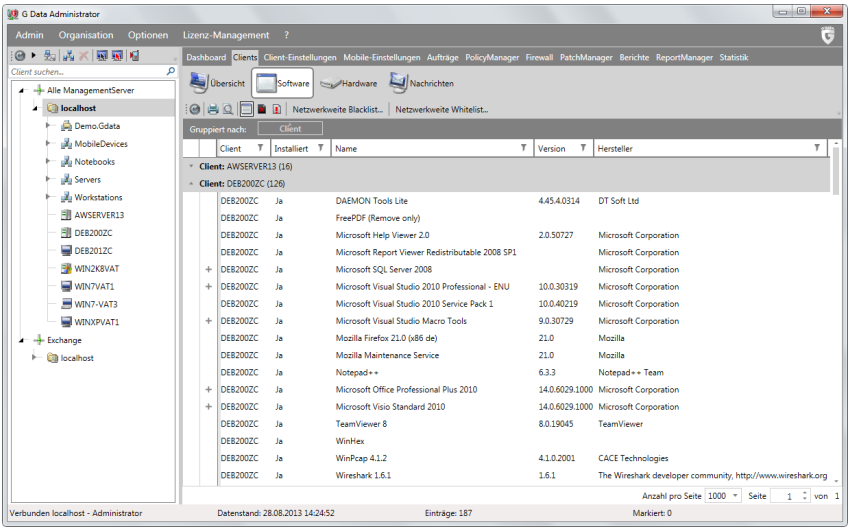


Im Eulas verwalten-Fenster werden alle verfügbaren Eulas aufgelistet. Um eine Eula hinzuzufügen, klicken Sie auf **Hinzufügen**. Im Eula erstellen-Fenster können Sie **Name**, **Sprache** und **Inhalt** der Vereinbarung definieren. Ein Klick auf **OK** fügt die Eula der Liste hinzu.

Um eine vorhandene Eula zu bearbeiten, wählen Sie diese in der Liste aus und klicken dann bitte auf **Ändern**. Um eine Eula zu entfernen, wählen Sie diese aus und klicken auf **Löschen**.

4.4.2.2. Software

Das Software-Inventar erlaubt Ihnen, die Software-Nutzung im gesamten Netzwerk zu überwachen. Software kann dabei auf Blacklists oder Whitelists hinzugefügt werden, um Software-Management im Netzwerk zu unterstützen.



Die Übersicht können Sie mit folgenden Schaltflächen beeinflussen:

Aktualisieren

Drucken: Hiermit starten Sie den Druckvorgang für die Software-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details Sie ausdrucken möchten.

Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.

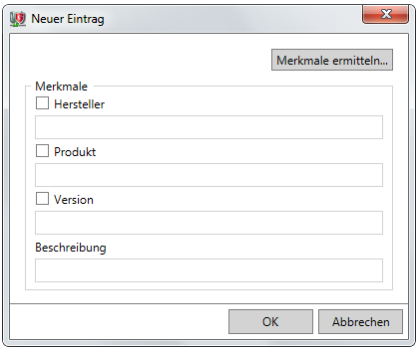
Alle anzeigen: Hiermit wird Ihnen sämtliche im Netzwerk auf den Clients installierte Software angezeigt.

Nur Software auf der Blacklist anzeigen: Über diese Einstellung können Sie sich die Software anzeigen, die durch Ihren Eintrag auf der Blacklist auf den Clients nicht ausgeführt werden kann.

Nur Software anzeigen, die nicht auf der Whitelist ist: Hiermit erhalten Sie einen Überblick über installierte Software auf den Netzwerk-Clients, die

vom Netzwerkadministrator noch nicht überprüft und kategorisiert wurde. Mit Hilfe dieser Ansicht können Sie gefundene Software mit einem Rechtsklick auf die Whitelist oder Blacklist setzen.

In der Listenansicht wird installierte Software für alle Clients im Clientauswahlbereich aufgelistet. Um die Whitelist bzw. Blacklist zu füllen, klicken Sie bitte auf die Schaltfläche **Netzwerkweite Blacklist** bzw. **Netzwerkweite Whitelist** und in dem nun erscheinenden Fenster auf die Schaltfläche **Hinzufügen**. Über die Option **Merkmale ermitteln** können Sie Programme auswählen, die Sie auf eine Blacklist oder Whitelist setzen möchten und die zugehörigen Attribute eingeben, mit denen das jeweilige Programm ermittelt werden kann. Um ein Attribut als Regel zu nutzen, setzen Sie einfach das Häkchen an das entsprechende Kästchen. Auf diese Weise können Sie z.B. Software bestimmter Hersteller oder auch nur spezielle Programmversionen black- oder whitelisten. Wenn Ihnen die erforderlichen Daten zur Verfügung stehen, können Sie Software auch durch Direkteingabe der Merkmale (ohne Umweg über Merkmale ermitteln) auf die Black- oder Whitelist setzen.



Standardmäßig zeigt das Software-Inventar nur derzeit installierte Programme. Wählen Sie **Alle Filter zurücksetzen** um auch Programme zu zeigen, die zuvor installiert wurden, jetzt aber nicht mehr vorhanden sind.

4.4.2.3. Hardware

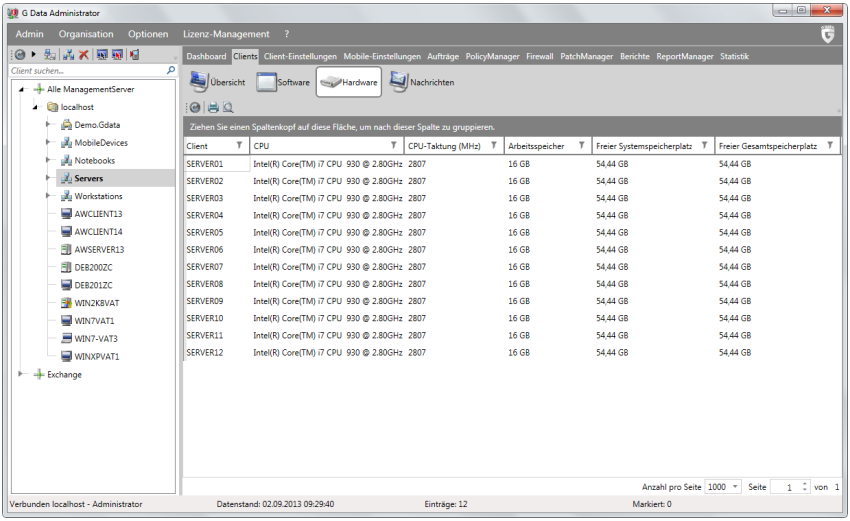
Über diese Ansicht erhalten Sie Informationen zu der von den Clients verwendeten Hardware.

Die Übersicht können Sie mit folgenden Schaltflächen beeinflussen.

Aktualisieren: Diese Funktion aktualisiert die Ansicht.

Drucken: Hiermit starten Sie den Druckvorgang für die Hardware-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details Sie ausdrucken möchten.

Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.


G Data Administrator
Admin
Organisation
Optionen
Lizenz-Management
?
Dashboard
Clients
Client-Einstellungen
Mobile-Einstellungen
Aufträge
PolicyManager
Firewall
PatchManager
Berichte
ReportManager
Statistik
Übersicht
Software
Hardware
Nachrichten
Client suchen...
Alle ManagementServer
localhost
Demo.Gdata
MobileDevices
Notebooks
Servers
Workstations
AWCLIENT13
AWCLIENT14
AWSERVER13
DEB200ZC
DEB201ZC
WIN2K8VAT
WIN7VAT1
WIN7-VAT3
WINXPVAT1
Exchange
Ziehen Sie einen Spaltenkopf auf diese Fläche, um nach dieser Spalte zu gruppieren.
Client
CPU
CPU-Taktung (MHz)
Arbeitsspeicher
Freier Systemspeicherplatz
Freier Gesamtspeicherplatz
SERVER01 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER02 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER03 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER04 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER05 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER06 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER07 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER08 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER09 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER10 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER11 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
SERVER12 Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz 2807 16 GB 54,44 GB 54,44 GB
Anzahl pro Seite 1000
Seite 1 von 1
Verbunden localhost - Administrator
Datenstand: 02.09.2013 09:29:40
Einträge: 12
Markiert: 0

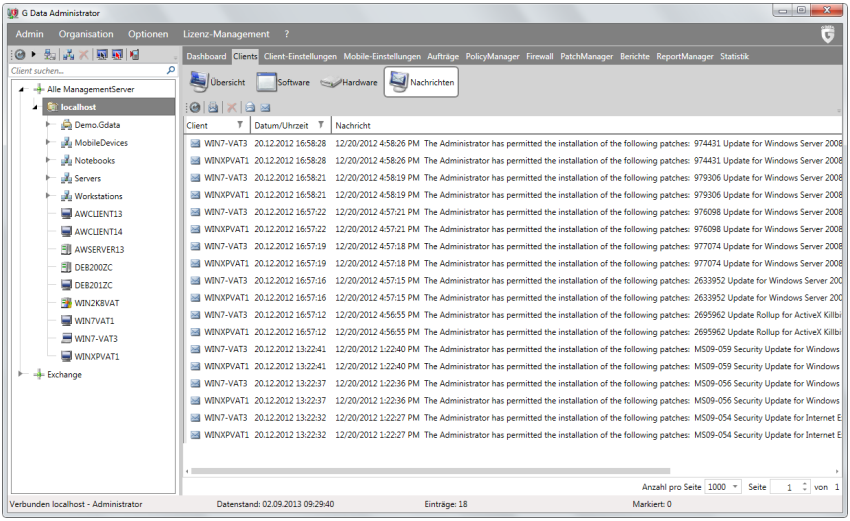
Mit einem rechten Mausklick auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zur Software zu- oder abwählen:

- **Client**
- **CPU**
- **CPU-Taktung (MHz)**
- **Arbeitsspeicher**
- **Freier Systemspeicherplatz**
- **Systemspeicherplatz (Statistik)**
- **Freier Gesamtspeicherplatz**
- **Gesamtspeicherplatz (Statistik)**
- **Systemhersteller**
- **Systemname**
- **Systemversion**
- **Systemfamilie**
- **CPU-ID**
- **Mainboardhersteller**
- **Mainboard**
- **Mainboardversion**
- **Bios-Hersteller**

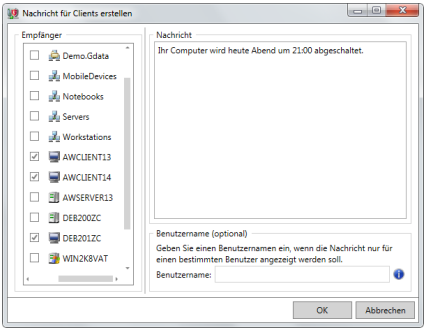
- **Bios Veröffentlichungsdatum**
- **Bios-Version**

4.4.2.4. Nachrichten

Sie können an einzelne Clients oder Client-Gruppen Nachrichten versenden. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert über Änderungen am Status des Clients informieren. Die Nachrichten werden dabei als Info unten rechts auf dem Desktop des Client-Rechners angezeigt.



Um eine neue Nachricht zu erzeugen, klicken Sie einfach mit der rechten Maustaste in die Spaltenansicht und wählen **Nachricht senden**. In dem nun erscheinenden Kontext-Dialog können Sie die Clients, denen Sie die Nachricht senden möchten, per Häkchen zu- oder abwählen.



Wenn Sie eine Nachricht nur bestimmten Benutzern eines Client-Rechners oder Netzwerks zugängig machen möchten, geben Sie dessen Anmeldenamen unter

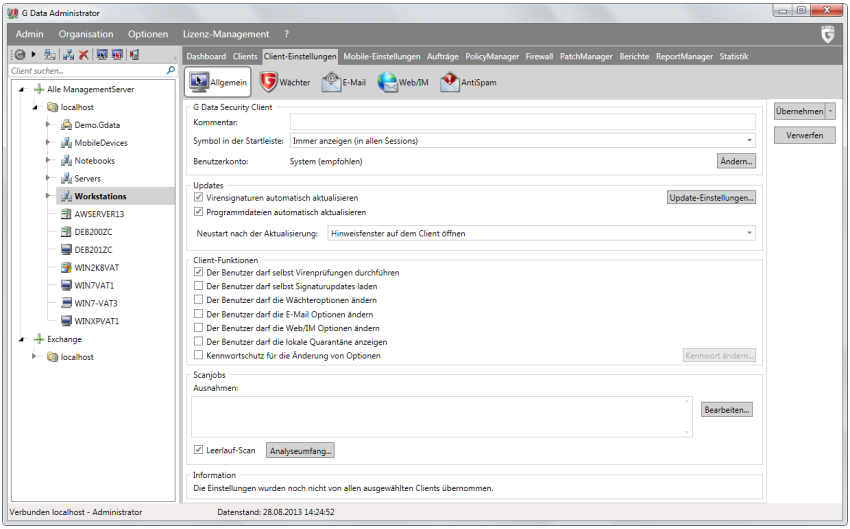
Benutzername ein. Tippen Sie nun in dem Feld **Nachricht** Ihre Hinweise für die Clients ein und drücken Sie dann auf die Schaltfläche **OK**.

4.4.3. Client-Einstellungen

In diesem Modul können Sie die Parameter für jeden einzelnen Client bzw. jede Gruppe von Clients managen. In dem Sie die Karteireiter Allgemein, Wächter, E-Mail, Web/IM und AntiSpam nutzen, können Sie Ihre Clients ganz individuell auf die Bedürfnisse Ihres Netzwerks und dessen Benutzer optimieren.

4.4.3.1. Allgemein

In diesem Bereich können Sie die grundlegenden Einstellungen der ausgewählten Clients bearbeiten.



G Data Security Client

Der G Data Security Client-Abschnitt behandelt die grundsätzliche Client-Funktionalität.

- **Kommentar**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Symbol in der Startleiste**: Für Terminal-Server und Windows mit schneller Benutzerumschaltung kann gewählt werden, in welchen Sessions ein Client-Symbol in der Taskleiste angezeigt werden soll: **Nie anzeigen**, **Nur in der ersten Session anzeigen** (für Terminalserver) oder **Immer anzeigen**. Bei normalen Clients kann mit der Option das Anzeigen des Client-Symbols wahlweise unterbunden werden. Damit der Anwender Zugriff auf erweiterte Client-Optionen, wie z.B. den Leerlauf-Scan hat, muss das Symbol angezeigt werden.

- **Benutzerkonto**: Die Client-Software läuft normalerweise im Systemkontext. Sie können hier ein anderes Konto angeben, um die Prüfung von Netzwerkverzeichnissen zu ermöglichen. Das Konto muss dazu Administratorrechte auf dem Client haben.

Updates

Im Bereich Updates können Sie die Update-Einstellungen für Virus-Signaturen und Programmdateien vornehmen.

- **Virensignaturen automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem ManagementServer vorhanden sind. Liegen aktualisierte Virensignaturen vor, werden diese automatisch auf dem Client installiert.
- **Programmdateien automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Client-Programmdateien. Die Clients prüfen periodisch, ob aktualisierte Programmdateien auf dem ManagementServer vorhanden sind. Liegen aktualisierte Programmdateien vor, werden diese automatisch auf dem Client installiert. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss. Je nach Einstellung unter **Neustart nach der Aktualisierung** hat der Anwender auf dem Client die Möglichkeit, den Abschluss der Aktualisierung auf einen späteren Zeitpunkt zu verschieben.
- **Neustart nach der Aktualisierung**: Wählen Sie **Hinweisfenster auf dem Client öffnen** um den Anwender darüber zu unterrichten, dass er seinen Client-Rechner in nächster Zeit neu starten sollte, damit das Update eingespielt werden kann. **Bericht erzeugen** erzeugt einen Bericht im Bereich **Berichte**. Über die Funktion **Neustart ohne Abfrage durchführen** wird auf dem Client-Rechner ungefragt automatisch ein Neustart durchgeführt.
- **Update-Einstellungen**: Hier wird festgelegt, woher die Clients ihre Virensignaturupdates beziehen. Standardmäßig laden Clients die Virensignaturen vom ManagementServer herunter. Dazu prüfen sie zu jedem Synchronisationsintervall, ob neue Signaturen vorliegen. Alternativ können die Virensignaturen von den G Data UpdateServern heruntergeladen werden. Für mobile Arbeitsplätze empfiehlt sich als weitere Alternative der Mischbetrieb, d.h. solange der Client eine Verbindung zum ManagementServer hat, bezieht er die Aktualisierungen von dort. Besteht hingegen keine Verbindung zum ManagementServer, werden die Virensignaturen automatisch aus dem Internet heruntergeladen. Die genannten Alternativen können über die Schaltfläche **Einstellungen und Zeitplanung** konfiguriert werden.

Client-Funktionen

Im Folgenden werden die Berechtigungen vergeben, die der Benutzer lokal für einzelne Clientfunktionen hat. So können dem Anwender umfangreiche oder auch nur stark eingeschränkte Rechte zur Änderung von Einstellungen eingeräumt werden

- **Der Benutzer darf selbst Virenprüfungen durchführen**: Im akuten Verdachtsfall kann der Anwender wie bei einer lokal installierten Antivirenlösung auf seinem Rechner unabhängig vom ManagementServer eine Virenprüfung durchführen. Ergebnisse dieser Virenprüfung werden beim nächsten Kontakt mit dem ManagementServer an diesen übermittelt. Diese Funktion erlaubt auch Änderungen im Bereich Virenprüfung (lokale Einstellungen).
- **Der Benutzer darf selbst Signaturupdates laden**: Wenn Sie diese Funktion aktivieren, darf der Nutzer des Clientrechners aus dem Kontextmenü heraus Virensignaturen auch ohne Verbindung zum ManagementServer direkt aus dem Internet laden.
- **Der Benutzer darf die Wächteroptionen ändern**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen im Bereich **Wächter** zu ändern.
- **Der Benutzer darf die E-Mail Optionen ändern**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen in den Bereichen **Email** und **AntiSpam** zu ändern.
- **Der Benutzer darf die Web/IM Optionen ändern**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen im Bereich **Web/IM** zu ändern.
- **Der Benutzer darf die lokale Quarantäne anzeigen**: Wenn das Anzeigen der lokalen Quarantäne erlaubt wird, kann der Anwender Daten, die vom Wächter wegen Virenbefall oder -verdacht in Quarantäne geschoben wurden ggf. desinfizieren, löschen oder zurückbewegen. Beachten Sie dabei, dass bei einem Zurückbewegen einer Datei aus der Quarantäne ein Virus nicht entfernt wird. Diese Option sollte deshalb nur versierten Anwendern auf den Clients zugänglich gemacht werden.
- **Kennwortschutz für die Änderung von Optionen**: Um einer missbräuchlichen Manipulation von lokalen Einstellungen vorzubeugen, gibt es die Möglichkeit, die Änderung von Optionen nur dann zuzulassen, wenn ein Passwort eingegeben wird. So lässt sich beispielsweise verhindern, dass ein User die Einstellungen ändert. Das Passwort kann individuell für den jeweiligen Client oder die jeweilige Gruppe vergeben werden; darauf muss nur den autorisierten Nutzern dieses Passwort mitgeteilt werden.

Scanjobs

Sie können hier Ausnahmen definieren, die nicht während der Ausführung der Scan-Aufträge überprüft werden. Zum Beispiel können Archiv- und Backup-Bereiche einer Festplatte oder Partition als Ausnahmen definiert werden, auch bestimmte Ordner oder sogar Dateierweiterungen können von den Scanjobs ausgeschlossen werden. Diese Ausnahmen können auch für komplette Gruppen definiert werden. Falls die Clients in einer Gruppe unterschiedliche Ausnahmeverzeichnisse definiert haben, können neue Verzeichnisse hinzugefügt oder vorhandene gelöscht werden. Die speziell für einzelne Clients definierten Verzeichnisse bleiben dabei erhalten. Das gleiche Verfahren wird

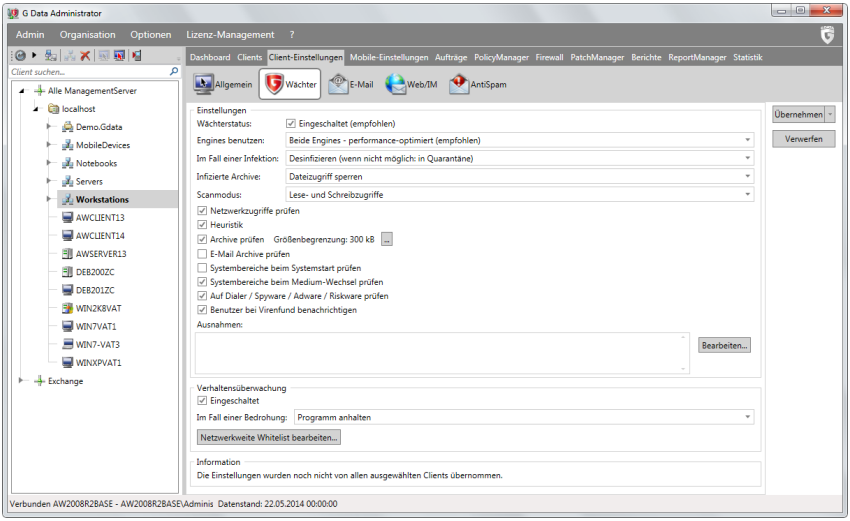
auch bei den Wächterausnahmen angewendet.

Wenn Sie möchten, dass der Client einen Virenscan durchführen soll, wenn sich der Computer im Leerlauf befindet, wählen Sie die Option **Leerlauf-Scan**. Durch Anklicken der **Analyseumfang**-Schaltfläche können Sie den Scan-Bereich festlegen. Standardmäßig sind hier alle lokalen Festplattenlaufwerke eingestellt.

> Besonderheit auf einem Linux-Fileserver: Bei der Auswahl von Ausnahmeverzeichnissen werden das Root-Laufwerk (/) und alle Freigaben zurückgeliefert. Dabei können Laufwerks-, Verzeichnis- und Dateiausnahmen angelegt werden.

4.4.3.2. Wächter

Hier können die Wächtereinstellungen vorgenommen werden. Der Wächter sollte grundsätzlich nicht deaktiviert werden, da dieser für den Echtzeitschutz vor Schädlingen sorgt. Wird der Wächter deaktiviert, besteht dieser Schutz nicht mehr. Es wird daher empfohlen, den Wächter nur dann auszuschalten, wenn ein berechtigtes Interesse daran besteht, zum Beispiel Fehlersuche oder Diagnose.



Die Definition von Ausnahmen für den Wächter ist möglich. Sollte eine Anwendung durch den Einsatz des Wächters mit Performanceeinbußen zu kämpfen haben, können für die entsprechenden Programmdateien, Prozesse oder Dateien Ausnahmen hinzugefügt werden; ausgenommene Dateien werden dann nicht mehr vom Wächter geprüft. Beachten Sie, dass das Hinzufügen von Wächterausnahmen unter Umständen ein Sicherheitsrisiko darstellen kann.

Einstellungen

Wächter-Einstellungen können dazu genutzt werden, um Scans zu konfigurieren und Ausnahmen zu definieren.

- **Wächterstatus**: Hier können Sie den Wächter anschalten bzw. ausschalten. Generell sollten Sie den Wächter eingeschaltet lassen. Er ist die Grundlage für einen permanenten und lückenlosen Virenschutz.
- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich.
- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
  - **Dateizugriff sperren**: Auf eine infizierte Datei können weder Schreib- noch Lesezugriffe ausgeführt werden.
  - **Desinfizieren (wenn nicht möglich: Zugriff sperren)**: Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, wird der Dateizugriff gesperrt.
  - **Desinfizieren (wenn nicht möglich: in Quarantäne)**: Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei in die Quarantäne verschoben.
  - **Desinfizieren (wenn nicht möglich: Datei löschen)**: Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei gelöscht. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.
  - **Datei in Quarantäne verschieben**: Hier wird die infizierte Datei in die Quarantäne verschoben. Eine mögliche Desinfektion der Datei kann dann manuell durch den Systemadministrator durchgeführt werden.
  - **Infizierte Datei löschen**: Als rigorose Maßnahme hilft diese Funktion dabei, den Virus wirkungsvoll einzudämmen. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte Archive behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Scanmodus**: Legen Sie hier fest, wie Dateien gescannt werden sollen. **Lesezugriffe** scannt jede Datei sofort, wenn Sie gelesen wird. **Lese- und Schreibzugriffe** überprüft Dateien nicht nur bei Lese- sondern auch bei Schreibzugriffen. Dies dient als Schutz vor Viren, die möglicherweise von einem anderen ungeschützten Client oder aus dem Internet kopiert werden. **Bei Ausführung** führt einen Scan durch, sobald eine Datei ausgeführt wird.

- **Netzwerkzugriffe prüfen**: Hier können Sie die Vorgehensweise des Wächters im Zusammenhang mit Netzwerkzugriffen festlegen. Wenn Sie ihr gesamtes Netzwerk generell mit der G Data Software überwachen, kann eine Überprüfung der Netzwerkzugriffe entfallen.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale erkannt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann in seltenen Fällen auch ein Fehlalarm erzeugt werden.
- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der G Data Virenwächter auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfen großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen**: Diese Option sollte in der Regel ausgeschaltet werden, da die Prüfung von E-Mail-Archiven in der Regel sehr lange dauert und im Falle einer infizierten Mail eine Mailbox - abhängig von den Einstellungen des Virenscans - in die Quarantäne verschoben oder gelöscht wird. Alle Mails innerhalb des Mailarchivs wären in einem solchen Fall nicht mehr verfügbar. Da der Wächter die Ausführung von infizierten E-Mail-Anhängen blockiert, wird durch das Ausschalten dieser Option kein Sicherheitsloch geschaffen. Bei der Verwendung von Outlook werden die ein- und ausgehenden Mails zusätzlich durch ein integriertes Plugin geprüft.
- **Systembereiche beim Systemstart/Medium-Wechsel prüfen**: Systembereiche (z.B. Bootsektoren) Ihres Computers sollten nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue DVD o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit der G Data Software können Sie Ihr System auch auf Dialer und andere Schadprogramme (Spyware, Adware, Riskware) überprüfen. Hierbei handelt es sich z.B. um Programme, die unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen. Spyware kann z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Benutzer bei Virenfund benachrichtigen**: Wird diese Option aktiviert, öffnet sich bei einem Virenfund durch den Wächter auf dem betroffenen Client ein Hinweisfenster, das den Benutzer darüber in Kenntnis setzt, dass auf seinem System ein Virus gefunden wurde. Die gefundene Datei sowie der Pfad und die Bezeichnung des gefundenen Schädlings werden dort angezeigt.

Unter **Ausnahmen** können Sie beim Client die Virenprüfung auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können Sie z.B. Ordner mit selten benötigten Archiven aussparen, um diese in einem gesonderten Scanauftrag zu prüfen. Des Weiteren lassen sich bestimmte Dateien und Dateitypen von der Virenprüfung ausschließen. Folgende Ausnahmen sind möglich:

- **Verzeichnis**: Wählen Sie hier mit dem Anklicken der Verzeichnis-Schaltfläche einen Ordner (gegebenenfalls inkl. seiner darin befindlichen Unterordner) aus, der nicht vom Wächter kontrolliert werden soll.
- **Laufwerk**: Wählen Sie hier mit Anklicken der Verzeichnis-Schaltfläche ein Laufwerk (Partition, Festplatte) aus, welches Sie vom Wächter nicht kontrollieren lassen möchten.
- **Datei**: Hier können Sie den Namen der Datei eingeben, die Sie von der Wächterkontrolle ausnehmen möchten. Sie können hier auch mit Platzhaltern arbeiten.
- **Prozess**: Soll ein bestimmter Prozess nicht vom Wächter überwacht werden, sind das Verzeichnispfad und der Name des betreffenden Prozesses hier einzutragen.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und im Wächter Ausnahmen-Fenster vorhandene Ausnahmen auch wieder löschen oder modifizieren.

> Die Funktionsweise von Platzhaltern ist folgendermaßen: Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen. Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen. Um z.B. sämtliche Dateien mit der Dateiendung exe schützen zu lassen, geben Sie also *.exe ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu schützen (z.B. xlr, xls), geben Sie einfach *.xl? ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise text*.* ein. Dies würde die Dateien text1.txt, text2.txt, text3.txt usw. betreffen.

Verhaltensüberwachung

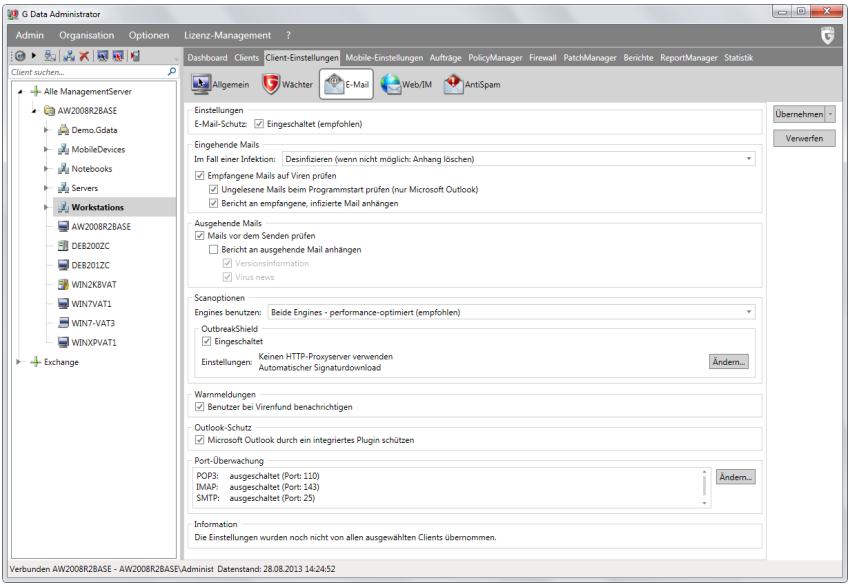
Die Verhaltensüberwachung stellt einen weiteren Schutz vor schädlichen Dateien und Prozessen dar, der im Unterschied zum Wächter, nicht signaturbasiert arbeitet, sondern das tatsächliche Verhalten eines Prozesses analysiert. Um eine Einordnung vorzunehmen, legt die Verhaltensüberwachung verschiedene Kriterien zugrunde, unter anderem Schreibzugriffe auf die Registry und das eventuelle Anlegen von Autostarteinträgen. Sind genügend Merkmale vorhanden, die den Schluss zulassen, dass ein Programm zumindest verdächtiges Verhalten an den Tag legt, wird die unter **Im Fall einer Bedrohung** eingestellte Aktion durchgeführt. Hierbei stehen die Optionen **Nur protokollieren**, **Programm anhalten** sowie **Programm anhalten und in Quarantäne verschieben** zur Verfügung.

Wenn die Verhaltensüberwachung eine Aktion durchführt, wird immer ein Bericht zu dem **Berichte**-Modul hinzugefügt. Falls ein Programm fälschlicherweise als Bedrohung identifiziert wurde, kann der jeweiligen Bericht benutzt werden, um einen Whitelist-

Eintrag zu erstellen. Whitelist-Einträge können über die Schaltfläche **Netzwerkweite Whitelist bearbeiten** angesehen und gelöscht werden.

4.4.3.3. E-Mail

Auf jedem G Data Security Client kann ein gesonderter Virenschutz für E-Mails eingerichtet werden. Hierbei werden Standardports für die Protokolle POP3, IMAP und SMTP überwacht. Für Microsoft Outlook findet darüber hinaus ein spezielles Plugin Verwendung. Das Plugin überprüft automatisch alle eingehenden Mails auf Viren und verhindert, dass infizierte Mails versendet werden.



Eingehende Mails

Der Bereich Eingehende Mails definiert Optionen für das Scannen eingehender E-Mails.

- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
- **Empfangene Mails auf Viren prüfen**: Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die den Client online erreichen.
- **Ungelesene Mails beim Programmstart prüfen (nur für Microsoft Outlook)**: Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die den Client erreichen, während dieser nicht mit dem Internet verbunden ist. Sobald Outlook geöffnet wird, werden deshalb sämtliche ungelesene Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern kontrolliert.
- **Bericht an empfangene, infizierte Mails anhängen**: Sobald eine an den

Client geschickte E-Mail einen Virus enthält, erhalten Sie im Body dieser Mail unter dem eigentlichen Mailtext die Meldung *ACHTUNG! Diese Mail enthält folgenden Virus* gefolgt vom Namen des Virus. Außerdem finden Sie vor dem eigentlichen Betreff die Mitteilung *[VIRUS]*. Sollten Sie die Option **Anhang/Text löschen** aktiviert haben, wird Ihnen außerdem mitgeteilt, dass der infizierte Teil der E-Mail gelöscht wurde.

Ausgehende Mails

Der Bereich Ausgehende Mails definiert Optionen für das Scannen ausgehender E-Mails.

- **Mails vor dem Senden prüfen**: Damit aus Ihrem Netzwerk keine Viren per Mail verschickt werden, bietet die G Data Software auch die Möglichkeit, Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollte tatsächlich ein Virus versendet werden, erscheint die Meldung *Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname]*. Die entsprechende E-Mail wird nicht versandt.
- **Bericht an ausgehende Mails anhängen**: Ein Prüfbericht wird im Body jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Dieser lautet *Virengeprüft von G Data AntiVirus*, so lange Sie die Option **Mails vor dem Senden prüfen** aktiviert haben. Zusätzlich können Sie hier das Versionsdatum von G Data AntiVirus (**Versionsinformation**) angeben.

Scanoptionen

Der Bereich Scanoptionen konfiguriert die Scan-Parameter für eingehende und ausgehende E-Mails.

- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten, den so genannten Engines. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann eine Analyse schneller durchgeführt werden.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Unter **Ändern** können Sie festlegen, ob das OutbreakShield zur Steigerung der Erkennungsleistung zusätzliche Signaturen verwendet. Außerdem können Sie hier Zugangsdaten für die Internetverbindung oder einen Proxyserver eingeben, die dem OutbreakShield automatische Signaturdownloads aus dem Internet ermöglichen.

Warnmeldungen

Der Bereich Warnmeldungen konfiguriert Warnmeldungen für die Empfänger infizierter E-Mails.

- **Benutzer bei Virenfund benachrichtigen**: Sie können den Empfänger einer infizierten Nachricht automatisch informieren. Auf seinem Desktop wird dann eine Virenmeldung angezeigt.

Outlook-Schutz

Outlook-Schutz ermöglicht E-Mail-Scans in Outlook mit Hilfe eines integrierten Plugins.

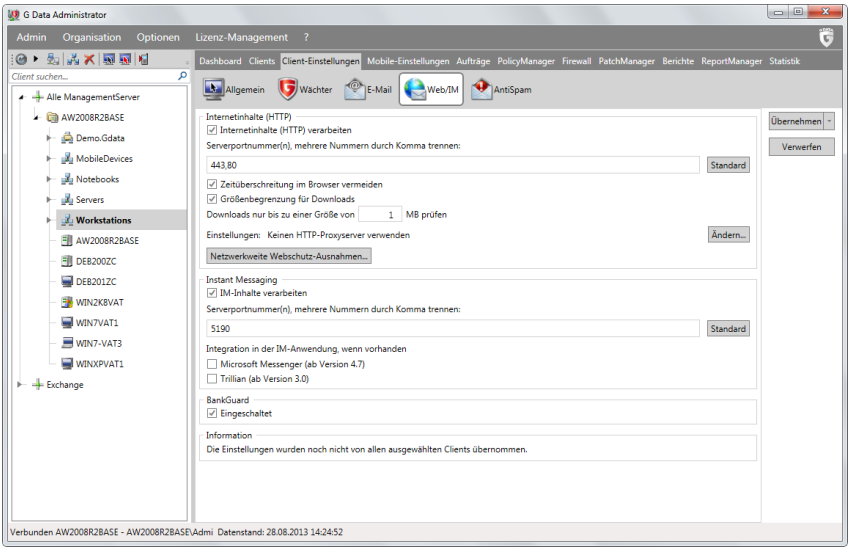
- **Microsoft Outlook durch ein integriertes Plug-In schützen**: Mit Aktivierung dieser Funktion wird in das Outlook des Clients im Menü **Extras** eine neue Funktion namens **Ordner auf Viren prüfen** eingefügt. Unabhängig von den G Data Administrator-Einstellungen kann der Nutzer des einzelnen Clients den jeweils momentan ausgewählten Mailordner nach Viren durchsuchen. Im Ansichtsfenster einer E-Mail können Sie im Menü **Extras** über **Mail auf Viren prüfen** eine Virenprüfung der Dateianlagen durchführen. Nach Abschluss des Vorgangs erscheint ein Info-Bildschirm, in dem das Ergebnis der Virenprüfung zusammengefasst wird. Hier erfahren Sie, ob die Virenanalyse vollständig erfolgte, erhalten Infos über die Anzahl der untersuchten Mails und Dateianhänge, etwaige Lesefehler sowie über gefundene Viren und wie damit verfahren wurde. Beide Fenster können Sie mit einem Klick auf die Schaltfläche Schließen ausblenden.

Port-Überwachung

Generell werden die Standardports für POP3 (110), IMAP (143) und SMTP (25) überwacht. Sollten die Porteinstellungen in Ihrem System davon abweichen, können Sie dies entsprechend anpassen.

4.4.3.4. Web/IM

In diesem Bereich können Sie Scan-Einstellungen für Internet, Instant Messaging und Online-Banking definieren. Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift der **Virenwächter** ein, wenn auf heruntergeladene, infizierte Dateien zugegriffen wird. Das System auf dem jeweiligen Client ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.



Internetinhalte (HTTP)

Der Bereich Internetinhalte (HTTP) behandelt Scan-Einstellungen für den HTTP-Datenverkehr.

- **Internetinhalte (HTTP) verarbeiten**: In den Web-Optionen können Sie bestimmen, dass sämtliche HTTP-Webinhalte schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Wird im Netzwerk ein Proxy für den Zugang zum Internet genutzt, muss der Serverport eingetragen werden, den der Proxy nutzt. Sonst ist eine Überprüfung des Internetverkehrs nicht möglich. Auch die **Web-Inhaltskontrolle** (verfügbar in der G Data EndpointProtection) benutzt diese Einstellungen.
- **Zeitüberschreitung im Browser vermeiden**: Da die G Data Software die Webinhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die angeforderten Daten erhält, da diese zunächst von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird diese Fehlermeldung unterdrückt. Sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann an den Internet Browser weitergereicht.
- **Größenbegrenzung für Downloads**: Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte aussetzen. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Download größerer Dateien nicht zu Verzögerungen durch die Virenkontrolle kommt.

- **Netzwerkweite Webschutz-Ausnahmen**: Diese Funktion erlaubt es Ihnen, bestimmte Webseiten generell von der Überprüfung durch den Webschutz auszunehmen.

Instant Messaging

Der Bereich Instant Messaging behandelt Scan-Einstellungen für Instant Messaging-Datenverkehr.

- **IM-Inhalte verarbeiten**: Da auch über Instant Messaging-Programme Viren und andere Schadprogramme verbreitet werden, kann die G Data Software auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten die verwendeten Instant Messaging-Anwendungen nicht die Standardports nutzen, geben Sie unter **Serverportnummer(n)**, die entsprechenden Ports ein.
- **Integration in der IM-Anwendung**: Sollten Sie den Microsoft Messenger (ab Version 4.7) oder Trillian (ab Version 3.0) verwenden, steht durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü zur Verfügung, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

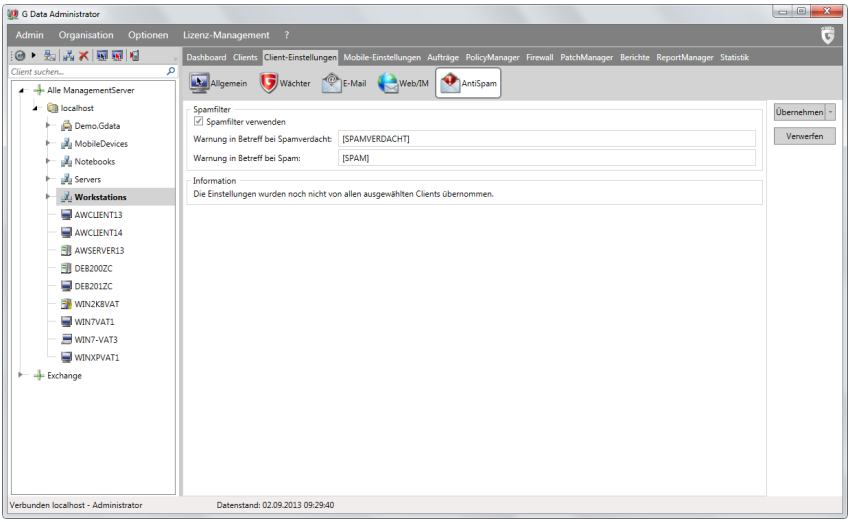
BankGuard

Banking-Trojaner werden zu einer immer größeren Bedrohung. Die wegweisende Technologie von G Data BankGuard sichert Bankgeschäfte von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G Data BankGuard sicher, dass Internet-Browser nicht von einem Banking-Trojaner manipuliert werden. Durch diesen proaktiven Sofortschutz von mehr als 99 % sind Online-Bankgeschäfte bestmöglich geschützt - selbst vor bisher unbekannten Trojanern. BankGuard sollte für alle Clients aktiviert werden, die den Internet Explorer, Firefox und/oder Chrome nutzen.

4.4.3.5. AntiSpam

Wenn Sie das Häkchen bei **Spamfilter verwenden** setzen, wird der E-Mail-Verkehr des Clients auf eventuelle Spam-Mails überprüft. Sobald eine E-Mail als Spam erkannt wird oder unter Spamverdacht fällt, können Sie eine Warnung festlegen, die dann im Betreff der Mail angezeigt wird.

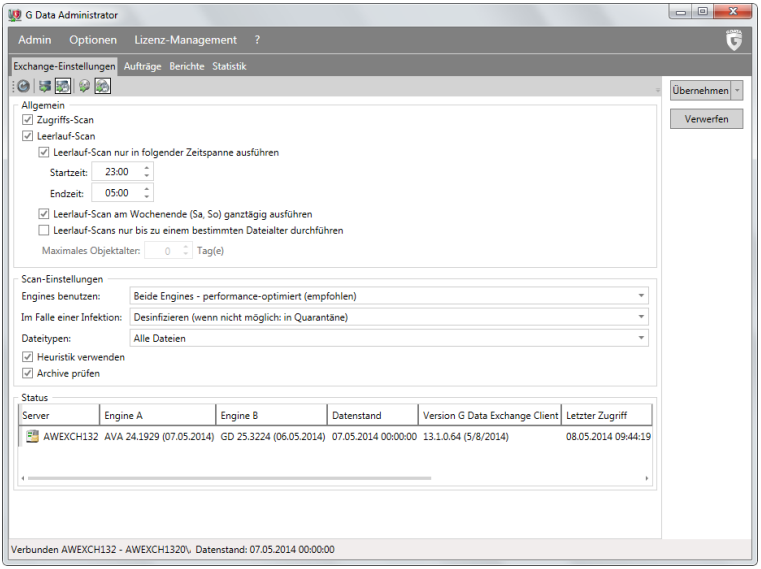
> Über die Warnung können Sie - oder der Anwender - auf dem Client im Mailprogramm eine Regel definieren, nach der z.B. Mails, die die Meldung *[Spam]* in der Betreffzeile haben, automatisch in einen speziellen Ordner für Spam- und Junk-Mail verschoben werden.



4.4.4. Exchange-Einstellungen

G Data MailSecurity ist als optionales Modul verfügbar.

Das MailSecurity Exchange-Plugin kann über den Aufgabenbereich Exchange-Einstellungen konfiguriert werden. Der Bereich wird aktiviert sobald das Plugin auf einem Exchange Server 2007 SP1, 2010 oder 2013 installiert worden ist und sich bei dem ManagementServer angemeldet hat.



Die Symbolleiste zeigt Update-Schaltflächen für Virensignaturen und Programmdateien. Wie bei normalen Clients benutzt das Exchange-Plugin Virensignaturen um Malware zu erkennen. Aktivieren Sie die Option **Virendatenbank automatisch aktualisieren**, um automatisch die neuesten Virensignaturen herunterzuladen. Das Plugin prüft dann bei jeder ManagementServer-Synchronisation, ob neue Virensignaturen vorliegen. Eine manuelle Update-Prüfung kann über die Option **Virendatenbank jetzt aktualisieren** gestartet werden. Beide Optionen sind auch verfügbar für Plugin-Programmdateien.

4.4.4.1. Allgemein

Der Bereich Allgemein beinhaltet Funktionen für Malware-Schutz. Sie können zwei verschiedene Schutzfunktionen benutzen: Automatische Prüfung und Leerlauf-Scan. Der **Zugriffs-Scan** prüft alle Mails, Anhänge und Objekte auf Malware, unmittelbar bevor sie von Exchange geöffnet werden. Im Fall einer Malware-Infektion werden die unter **Scan-Einstellungen** definierten Maßnahmen ausgeführt.

Zusätzlich oder als Ersatz für den Zugriffs-Scan können Sie den **Leerlauf-Scan** aktivieren. Der Leerlauf-Scan prüft Exchange-Objekte automatisch, sobald der Server im Leerlauf ist, um so eine Leistungsverminderung zu vermeiden. Wenn Exchange auf einem Server installiert wurde, auf dem auch andere Software ausgeführt wird (z.B. Datenbank- oder Web-Server), soll der Leerlauf-Scan nur in einer bestimmten Zeitspanne ausgeführt werden. Damit wird sichergestellt, dass die Leistung anderer Server-Prozesse nicht von dem Scan eingeschränkt wird.

- **Leerlauf-Scan nur in folgender Zeitspanne ausführen**: Geben Sie eine Start- und Endzeit ein, um den Leerlauf-Scan nur in einer bestimmten Zeitspanne auszuführen (z.B. nachts).
- **Leerlauf-Scan am Wochenende (Sa, So) ganztägig ausführen**: Der Leerlauf-Scan wird samstags und sonntags ganztägig ausgeführt.
- **Leerlauf-Scan nur bis zu einem bestimmten Dateialter durchführen**: Ältere Objekte können vom Leerlauf-Scan ausgeschlossen werden.

4.4.4.2. Scan-Einstellungen

Die Scan-Einstellungen für den Zugriffs-Scan und den Leerlauf-Scan ähneln den **Wächter**- und **Scanauftrag**-Einstellungen.

- **Engines benutzen**: Die Scans benutzen entweder einen oder beide Engines. Es wird empfohlen, beide Engines im performance-optimierten Modus zu benutzen.
- **Im Falle einer Infektion**: Das Exchange-Plugin kann infizierte Dateien auf mehrere Arten behandeln. Die empfohlene Option ist **Desinfizieren (wenn nicht möglich: in Quarantäne**).
- **Dateitypen**: Um Scans zu beschleunigen, können sie auf Programmdateien und Dokumente beschränkt werden. Es wird jedoch empfohlen, alle Dateien zu

überprüfen.

- **Heuristik verwenden**: Mithilfe von Heuristik kann Malware auf Basis von Verhalten erkannt werden.
- **Archive prüfen**: Archive können Malware beinhalten. Wenn eine oder mehrere Dateien innerhalb eines Archives infiziert sind, wird das Archiv als Ganzes desinfiziert, in die Quarantäne geschoben oder entfernt, ggf. einschließlich sauberer Dateien.

4.4.4.3. Status

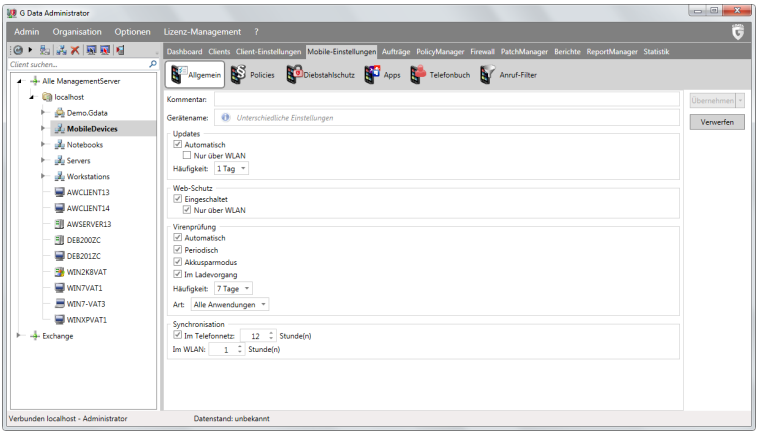
Der Status-Bereich zeigt Informationen über alle gewählten Exchange-Plugin-Clients. Die Daten ähneln den Informationen der Übersichtsliste im **Clients**-Modul: Die Zeit des letzten Zugriffs und Versionsinformationen des Plugins sowie beider Engines. Die Übersicht kann über die Symbolleiste manuell aktualisiert werden, indem Sie die Schaltfläche **Aktualisieren** wählen.

4.4.5. Mobile-Einstellungen

Die Mobile Einstellungen-Registerkarte bietet einfachen Zugang zu den Möglichkeiten des G Data Administrators, mobile Geräte zu administrieren. Nachdem auf einem oder mehreren Android-Geräten die G Data Internet Security installiert wurde, erscheinen diese als Clients im Clientauswahlbereich. Das Auswählen eines mobilen Clients oder einer Gruppe mit mobilen Clients ermöglicht dann den Zugriff zu der Registrierkarte Mobile-Einstellungen.

4.4.5.1. Allgemein

Die Registerkarte Allgemein bietet Einstellungen für automatische Updates, Web-Schutz, Virenprüfung und Synchronisation sowie zwei allgemeine Geräte-Management-Optionen.



- **Kommentar**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Gerätename**: Geben Sie hier einen Gerätenamen ein.

Updates

Der Abschnitt Updates deckt Einstellungen in Bezug auf Updates ab.

- **Automatisch**: Hier können Sie festlegen, ob der mobile Client automatisch nach Software- und Virensignaturen suchen soll. Wenn Updates nicht automatisch heruntergeladen werden sollen, kann der Benutzer diese trotzdem noch manuell aktualisieren. Falls Sie sich für eine automatische Aktualisierung entscheiden, können Sie des Weiteren festlegen, wie oft dies zu erfolgen hat und ob eine Aktualisierung über das Mobilfunknetz oder nur über WLAN erfolgen soll.

Web-Schutz

Der Web-Schutz-Abschnitt umfasst die Möglichkeit, den Web-Schutz auf WLAN-Netze zu begrenzen.

- **Eingeschaltet**: Legen Sie hier fest, ob mobile Geräte beim Zugriff aufs Internet vom Web-Schutz geschützt werden sollen. Dies kann wahlweise als genereller Schutz eingestellt werden oder nur wenn der Internetzugriff über WLAN erfolgt.

Virenprüfung

Der Bereich Virenprüfung ermöglicht Ihnen, Parameter für On-Demand-und On-Access-Virenscans zu definieren.

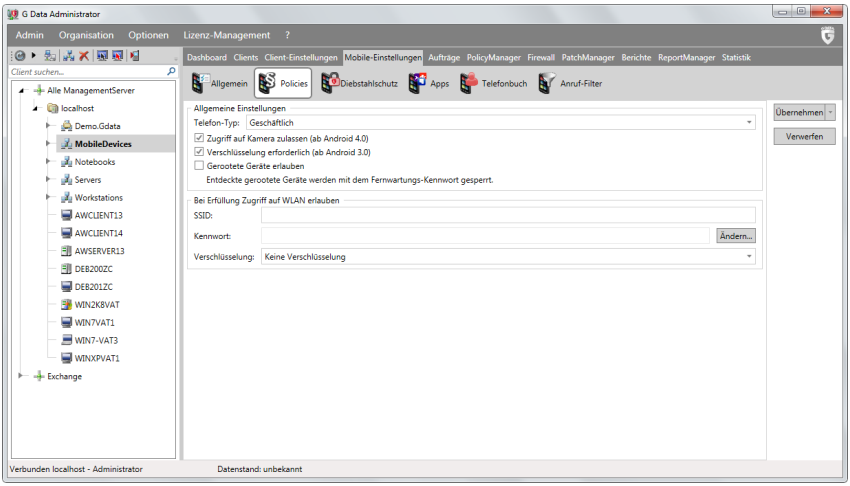
- **Automatisch**: Hier können Sie festlegen, dass neu installierte Applikationen automatisch überprüft werden.
- **Periodisch**: Hier können Sie einen periodischen Scan definieren. Aktivieren Sie dazu das Kontrollkästchen Periodisch und legen Sie dann die **Häufigkeit** fest.
- **Akkusparmodus**: Setzen Sie den periodischen Scan aus, solange Ihr Smartphone im Akkusparmodus läuft.
- **Im Ladevorgang**: Hier können Sie festlegen, dass der periodische Scan nur dann durchgeführt wird, wenn sich das Mobilgerät im Ladezustand befindet.
- **Art**: Hier können Sie festlegen, ob **Alle Anwendungen** gescannt werden sollen oder nur **Installierte Anwendungen**.

Synchronisation

Die Option Synchronisation legt fest, wie oft der mobile Client seine Daten mit dem ManagementServer synchronisiert. Geben Sie hier den Aktualisierungszyklus in Stunden an und entscheiden Sie, ob eine Synchronisation nur über WLAN oder auch über das Telefonnetz erfolgen soll.

4.4.5.2. Policies

Sie haben die Möglichkeit, Policies für verschiedene Handy-Typen zu definieren und damit Ihr Unternehmensnetzwerk zu schützen.



Allgemeine Einstellungen

Unter Allgemeine Einstellungen, wählen Sie den **Telefon-Typ** aus, zu dem das ausgewählte Gerät gehört. Für Geräte, die von Ihrem Unternehmen ausgegeben wurden, wählen Sie **Geschäftlich**. Damit sperren Sie diverse Einstellungsmöglichkeiten für den Benutzer, der diese dann nicht selber verändern kann. Ganz unabhängig vom Telefontyp können folgende Funktionen gesperrt werden:

- **Zugriff auf Kamera zulassen** (ab Android 4.0): ermöglicht den Zugriff auf die Handykamera (Android 4.0 und höher) abzuschalten
- **Verschlüsselung erforderlich** (ab Android 3.0): Hier muss die volle Geräteverschlüsselung aktiviert sein (Android 3.0 und höher)
- **Gerootete Geräte erlauben**: Erlauben oder verbieten Sie hier gerootete Geräte. Wenn die Funktion deaktiviert ist, werden gerootete Geräte mit dem Passwort blockiert, welches Sie unter **Diebstahlschutz** definiert haben. Außerdem wird gerooteten Geräten Zugriff auf das WLAN verweigert, welches Sie unter **Bei Erfüllung Zugriff auf WLAN erlauben** definiert haben.

Bei Erfüllung Zugriff auf WLAN erlauben

Der Zugang zu einem bestimmten WLAN-Netzwerk kann gerooteten Geräten untersagt werden. Dies ermöglicht Ihnen den Zugriff auf das Unternehmens-WLAN-Netzwerk nur für Geräte zu erlauben, die die Unternehmensrichtlinien erfüllen.

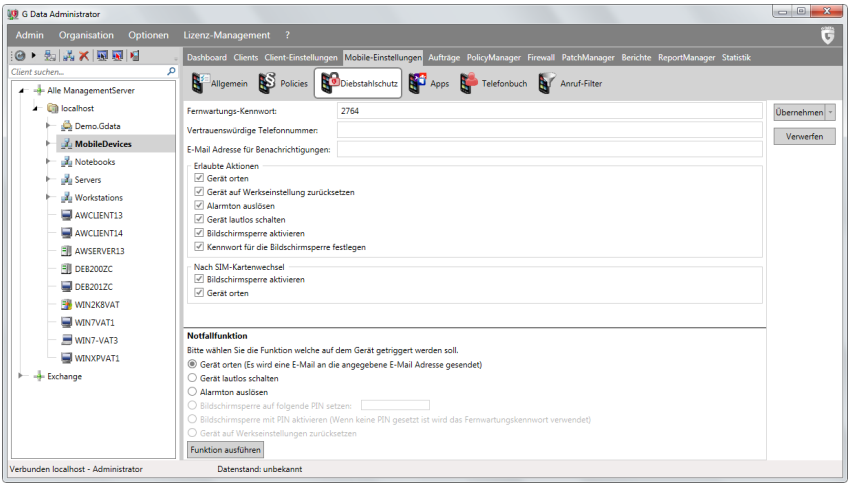
Geben Sie die **SSID** für das Firmennetzwerk ein, für das der Zugang aktiviert werden

soll. Wählen Sie die **Verschlüsselung** und vergeben Sie das **Kennwort** (wenn das Netzwerk verschlüsselt ist).

4.4.5.3. Diebstahlschutz

Um verlorene oder gestohlene Mobilgeräte zu schützen, bietet die Internet Security-App verschiedene Maßnahmen an, die ferngesteuert über SMS aktiviert werden können. Geräte, die gestohlen oder verloren werden, können aus der Ferne gesperrt, gelöscht oder lokalisiert werden. Diese Funktion aktivieren Sie durch das Senden einer SMS mit entsprechenden Befehlen an das verlorene Gerät. Über die Google Cloud Messaging-Funktion können diese Anti-Diebstahl-Funktionen auch jederzeit manuell ausgelöst werden.

Vor der Eingabe von Diebstahlschutz-Maßnahmen, sollten einige allgemeine Einstellungen vorgenommen werden. Das **Fernwartungs-Kennwort** (ein Zahlen-PIN-Code) ist notwendig, damit Sie sich per SMS bei Ihrem Smartphone identifizieren können. Auf diese Weise wird verhindert, dass andere Personen unauthorisiert Sperrbefehle oder dergleichen an Ihr Gerät senden. Ein weiteres Sicherheitsfeature ist eine **Vertrauenswürdige Telefonnummer**. Sie können das Fernwartungs-Kennwort ferngesteuert ändern, aber nur über die Telefonnummer welche Sie hier vorher eingegeben haben. Die **E-Mail Adresse für Benachrichtigungen** ist notwendig, um Antworten und Informationen zurück zu erhalten, die durch die SMS-Kommandos ausgelöst wurden (z.B. Standortinformationen).



Erlaubte Aktionen

Hier können Sie festlegen, welche Aktionen mit Ihrem Smartphone ausgeführt werden dürfen, sobald Sie diesem ein SMS-Kommando zuschicken. Setzen Sie hierzu Häkchen bei den Funktionen, die Sie aktivieren möchten:

- **Gerät orten**: Hiermit können Sie die Position des gestohlenen/verlorenen

Gerätes an die E-Mail-Adresse senden lassen, welche Sie vorher im Einstellungen-Bereich definiert haben. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: *Kennwort* **locate**.

- **Gerät auf Werkseinstellung zurücksetzen**: Hiermit können Sie Ihr gestohlenes/verlorenes Handy auf den Werkszustand zurücksetzen. Alle persönlichen Daten werden dabei gelöscht. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: *Kennwort* **wipe**.
- **Alarmton auslösen**: Über diese Funktion kann ein akustisches Signal abgespielt werden, bis Internet Security gestartet wird. Dies erleichtert das Auffinden eines verlorenen Handys. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: *Kennwort* **ring**.
- **Gerät lautlos schalten**: Wenn Sie nicht möchten, dass Ihr gestohlenes/ verlorenes Smartphone durch Klingel- oder Systemtöne auf sich aufmerksam macht, können Sie es hiermit lautlos stellen. Die Funktionalität des Signaltons zum Wiederfinden des Geräts wird dabei natürlich nicht beeinträchtigt. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: *Kennwort* **mute**.
- **Bildschirmsperre aktivieren**: Hiermit können Sie den Bildschirm Ihres gestohlenen/verlorenen Smartphones sperren. Eine Nutzung des Smartphones ist so nicht mehr möglich. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: *Kennwort* **lock**. Sollte kein Passwort vergeben worden sein, wird hier das Passwort verwendet, welches Sie im Bereich Einstellungen vergeben haben.
- **Kennwort für die Bildschirmsperre** festlegen: Damit Sie selber wieder Zugang zu Ihrem Smartphone erhalten, können Sie mit dieser Funktion ggf. das Kennwort für die Bildschirmsperre neu vergeben, wenn Sie das alte Passwort nicht mehr kennen. Zum Aktivieren dieses Kommandos verschicken Sie eine SMS mit dem Textinhalt: Kennwort **set device password:** *Gerätekennwort*.

Um das Fernwartungs-Kennwort ferngesteuert zu ändern, senden Sie eine SMS an Ihr Handy mit dem Gerät, wessen Nummer Sie unter **Vertrauenswürdige Telefonnummer** eingegeben haben. Das Kommand hierzu lautet: **remote password reset:** *NeuesKennwort*.

Nach SIM-Kartenwechsel

Bei der Installation der Internet Security-App merkt sich diese, welche SIM-Karte bei der Installation in dem Mobilgerät vorhanden war. Wenn diese Karte gewechselt wird, weil das Gerät z.B. gestohlen und weiterverkauft wurde, können automatisch bestimmte Aktionen erfolgen:

- **Bildschirmsperre aktivieren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Gerät orten**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.

Notfallfunktion

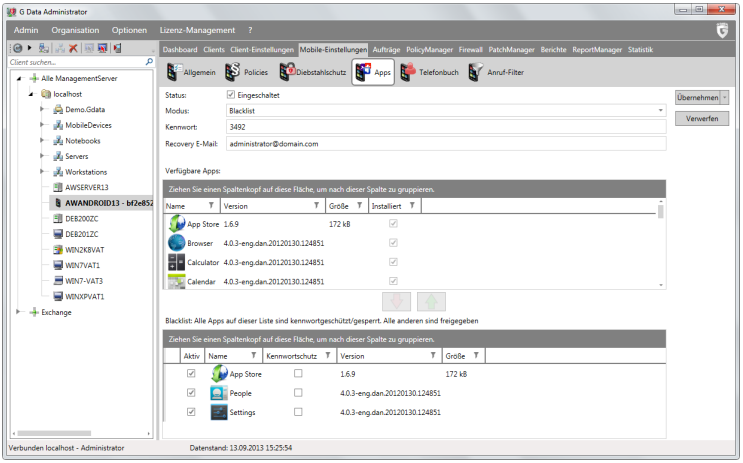
Mit dem Internet-basierten Google Cloud Messaging können Notfallmaßnahmen auf dem gestohlenen/verlorenen Mobilgerät ausgelöst werden. Diese funktionieren selbst dann, wenn das Mobilgerät ohne SIM-Karte genutzt wird. Vorher muss das Google Cloud Messaging allerdings konfiguriert werden: Geben Sie unter **Server-Einstellungen** > **Mobile** die **Sender-ID** und den **API-Key** ein. Wählen Sie dann die gewünschten Aktionen aus und klicken Sie auf Funktion ausführen, um den jeweiligen Befehl für die Aktion direkt an das Mobilgerät zu senden:

- **Gerät orten**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Gerät lautlos schalten**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Alarmton auslösen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Bildschirmsperre auf folgende PIN setzen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Bildschirmsperre mit PIN aktivieren**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.
- **Gerät auf Werkseinstellungen zurücksetzen**: Gleiche Funktionalität wie die Optionen unter **Erlaubte Aktionen**.

4.4.5.4. Apps

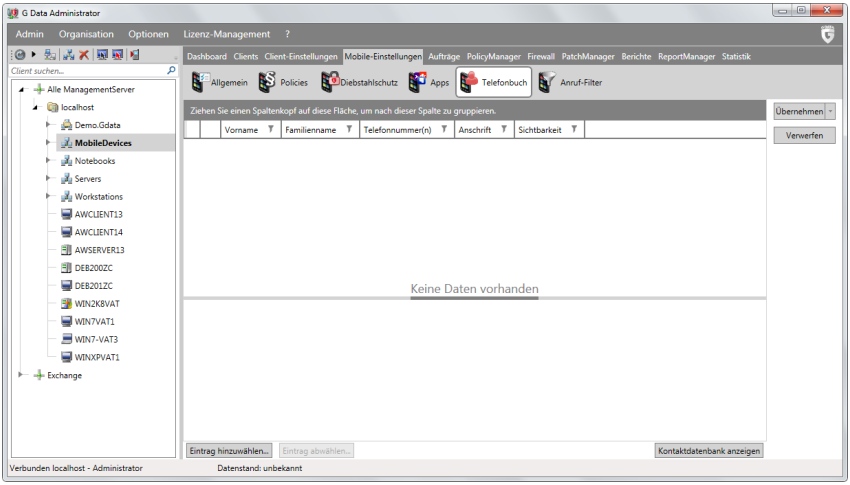
Das Apps-Panel ermöglicht Ihnen den Zugriff auf die App-Verwaltung Ihrer Mobilgeräte. Um Apps zu blockieren oder zu erlauben, müssen Sie zuerst entscheiden, ob der Filter für Apps im **Blacklist**- oder **Whitelist**-Modus verwendet werden soll. Im Blacklist-Modus werden nur bestimmte Apps, die auf einer Blacklist gelistet sind, blockiert oder ihr Zugriff wird über ein Passwort eingeschränkt. Beliebige andere Apps können verwendet werden. Im Whitelist-Modus werden nur die Apps zugelassen, die sich auch auf dieser Whitelist befinden. Das **Kennwort** (ein PIN-Code) wird dazu verwendet, auf gesperrte Apps zugreifen zu können. Außerdem können Sie eine **Recovery E-Mail** angeben, an die Sie sich das Kennwort zuschicken lassen können, falls Sie es vergessen haben.

Über **Verfügbare Apps** werden alle Apps aufgelistet, die auf dem jeweiligen Mobilgerät installiert wurden. Bei jeder App sehen Sie den **Namen** der App, die **Version** und die **Größe**. Über die Pfeiltasten können Sie Apps von der White- auf die Blacklist verschieben und andersherum. Hier können Sie auch den **Kennwortschutz** für entsprechend gelistete Apps vergeben.



4.4.5.5. Telefonbuch

Das Telefonbuch-Panel ermöglicht die erweiterte Verwaltung von Kontakten. Kontakte können in der Internet Security App einem Adressbuch hinzugefügt werden und sowohl die Kontakte, als auch ihre Kommunikation können im Mobilgerät so versteckt werden, dass diese nicht im normalen Adress- und Telefonbuch zu sehen sind. In Kombination mit diesen Funktionen kann das Telefonbuch der Internet Security-App das offizielle Android-Telefonbuch vollständig ersetzen.



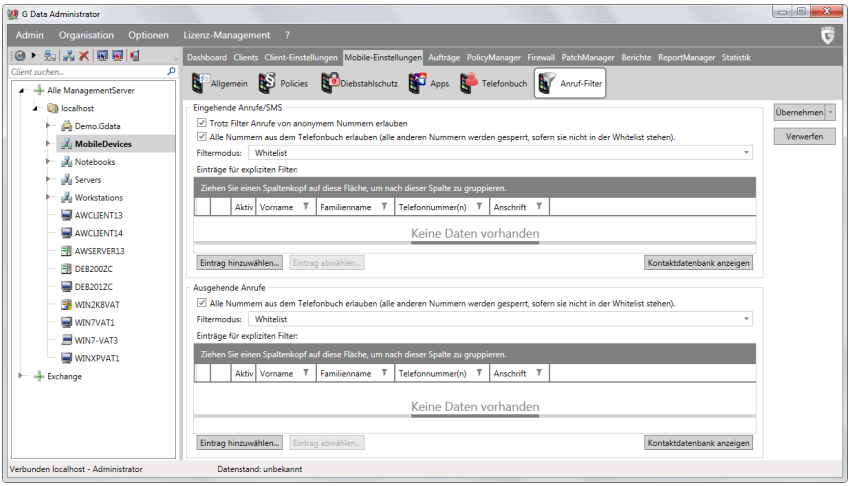
Die Hauptliste zeigt alle Kontakte, die dem Internet Security-Telefonbuch hinzugefügt wurden. Für jeden Kontakt sind die Felder **Vorname**, **Familienname**, **Telefonnummer(n)** und **Anschrift** aufgeführt. Über das Dropdown-Menü **Sichtbarkeit** können Sie festlegen, ob der jeweilige Kontakt im normalen Android-Telefonbuch angezeigt (**Sichtbar**) oder nicht angezeigt (**Versteckt**) wird. Darüber

hinaus können Sie alle Anrufe und SMS-Nachrichten der betreffenden Kontakte über **Kommunikation versteckt** verstecken. Um einen Kontakt zum Telefonbuch hinzuzufügen, klicken Sie auf **Eintrag hinzuwählen**. Im **Kontaktdatenbank**-Fenster werden alle Kontakte angezeigt, welche definiert wurden. Wählen Sie einen oder mehrere Kontakte aus und klicken Sie auf **Auswählen**, um die Kontakte dem Telefonbuch hinzuzufügen. Um einen Kontakt aus dem Telefonbuch zu entfernen, klicken Sie bitte **Eintrag abwählen**.

Um einen Kontakt in der Kontakt-Datenbank hinzuzufügen, klicken Sie auf die Schaltfläche **Kontakt erstellen** in der Symbolleiste oder **Kontakte importieren**, um Kontakte aus der Active Directory Organizational Unit (OU) heraus zu importieren. Beim Erstellen eines Kontakts, sollten Sie mindestens **Vorname** oder **Familienname** angeben. Darüber hinaus können Sie eine oder mehrere Postanschriften hinzufügen, sowie E-Mail-Adressen, Telefonnummern, Faxnummern und Organisationen. Um einen Kontakt aus der Kontakt-Datenbank zu entfernen, wählen Sie diesen aus und klicken Sie auf das **Löschen**-Symbol in der Symbolleiste oder wählen die Option **Löschen** im Kontextmenü.

4.4.5.6. Anruf-Filter

Der Anruf-Filter ermöglicht Ihnen, eingehende Anrufe und SMS-Nachrichten sowie ausgehende Anrufe zu filtern. Mit der gleichen Datenbank wie Sie im **Telefonbuch**-Panel verwendet wird, können Sie ganz einfach Kontakte zu einer Blacklist oder Whitelist hinzufügen, sowie generelle Filter definieren.



Eingehende Anrufe/SMS

Unter Eingehende Anrufe / SMS können Sie definieren, wie Internet Security mit eingehender Kommunikation umgehen soll. Deaktivieren Sie **Trotz Filter Anrufe von anonymen Nummern erlauben**, um alle anonymen Anrufe zu blockieren. Wenn Sie den zusätzlichen Filter **Alle Nummern aus dem Telefonbuch erlauben** wählen, wird

nur die Kommunikation mit Kontakten aus den Android- und Internet Security-Telefonbüchern erlaubt, sowie mit eventuellen Nummern auf der Whitelist.

Über die Funktion **Filtermodus** können Sie bestimmte Maßnahmen für eingehende Anrufe und SMS-Nachrichten definieren. Wählen Sie **Blacklist**, um die Kommunikation mit allen Kontakten zu erlauben, bis auf die, welche sich auf der Blacklist befinden oder wählen Sie **Whitelist**, um den Kontakt nur mit Kontakten zu erlauben, die auf der Whitelist gelistet sind. Durch das Anklicken von **Eintrag hinzuwählen**, können Sie jeden Kontakt aus der Kontakt-Datenbank zur jeweiligen Liste hinzuzufügen und über **Eintrag abwählen** aus der Liste entfernen.

Ausgehende Anrufe

Unter Ausgehende Anrufe können Sie definieren, wie Internet Security ausgehende Anrufe behandeln soll. Wenn Sie den zusätzlichen Filter **Alle Nummern aus dem Telefonbuch erlauben** wählen, können nur Kontakte aus den Android- und Internet Security-Telefonbüchern kontaktiert werden, sowie Kontakte auf der Whitelist.

Über die Funktion **Filtermodus** können Sie bestimmte Maßnahmen für eingehende Anrufe und SMS-Nachrichten definieren. Wählen Sie **Blacklist**, um die Kommunikation mit allen Kontakten zu erlauben, bis auf die, welche sich auf der Blacklist befinden oder wählen Sie **Whitelist**, um den Kontakt nur mit Kontakten zu erlauben, die auf der Whitelist gelistet sind. Durch das Anklicken von **Eintrag hinzuwählen**, können Sie jeden Kontakt aus der Kontakt-Datenbank zur jeweiligen Liste hinzuzufügen und über **Eintrag abwählen** aus der Liste entfernen.

Falls ein Benutzer versucht, eine gesperrte Nummer anzurufen, wird er über die Sperrung informiert und ihm wird die Möglichkeit angeboten, die Freigabe der Nummer anzufordern. Dieser Vorgang fügt einen Bericht im **Berichte**-Modul hinzu, über den der Administrator dann direkt einen Blacklist- oder Whitelist-Eintrag erstellen kann.

4.4.6. Aufträge

In diesem Aufgabenbereich werden Aufträge auf den G Data Clients definiert. Es gibt zwei unterschiedliche Auftragsarten: Einmalige Aufträge und periodische Aufträge. Die einmaligen Jobs werden einmal zum festgelegten Zeitpunkt ausgeführt, für die periodischen wird ein Zeitplan definiert, nach dem sie ausgeführt werden sollen. Sie können beliebig viele unterschiedliche Aufträge definieren. Generell ist es aus Gründen der Performance allerdings sinnvoll, dass sich Aufträge zeitlich nicht überschneiden. Als Aufträge bzw. Jobs werden alle Aufträge bezeichnet, die am G Data ManagementServer erstellt werden. Es kann sich hier um Scanaufträge, Backup- oder Wiederherstellungsaufträge handeln.

Im Aufgabenbereich Aufträge erscheinen alle Jobs unter den von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach folgenden Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet:

- **Name**: Der von Ihnen vorgegebene Name für den Job. Sie können hier beliebig lange Namen eingeben und auf diese Weise Ihren Job genau beschreiben, um bei vielen verschiedenen Jobs den Überblick zu behalten.
- **Client**: Hier finden Sie den Namen des jeweiligen Clients. Sie können Jobs nur für aktivierte Clients definieren.
- **Gruppe**: Sie können einzelne Clients zu Gruppen zusammenfassen, die dann dieselben Jobs nutzen. Wenn Sie einer Gruppe einen Job zuordnen, erscheinen in der Übersichtsliste nicht die einzelnen Rechner, sondern der Gruppenname.
- **Status**: Hier erhalten Sie den Status oder das Ergebnis eines Jobs im Klartext angezeigt. So erfahren Sie z.B., ob der Job gerade durchgeführt oder abgeschlossen wurde und werden auch darüber informiert, ob Viren gefunden wurden oder nicht.
- **Letzte Ausführung**: Über diese Spalte erhalten Sie Informationen darüber, wann der jeweilige Job das letzte Mal durchgeführt wurde.
- **Zeitintervall**: Gemäß der Zeitplanung, die Sie für jeden Job definieren können, steht hier, in welchem Turnus der Job wiederholt wird.
- **Umfang**: Hier erfahren Sie auf welche Datenträger (z.B. lokale Festplatten) sich die Analyse erstreckt.

Um Aufgaben zu verwalten, können Sie folgenden Optionen aus der Symbolleiste oberhalb der Aufgabenliste nutzen:

Aktualisieren

Löschen: Löscht alle markierten Jobs.

Einmaliger Scan-Auftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Rechner oder Rechnergruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Zeitplanung, Analyseumfang und weitere Scaneinstellungen festlegen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Scanaufträge**. Wählen Sie zum Ändern der Scan-Parameter im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**.

Periodischer Scan-Auftrag: Mit dieser Funktion lassen sich periodische Scanaufträge für einzelne Rechner oder Rechnergruppen definieren.

Backup-Auftrag: Definieren Sie hier, wann und in welchem Umfang die Daten auf Clients gebackupt werden sollen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Backupaufträge im Kapitel **Backupaufträge**. Backup-Funktionalitäten sind verfügbar als **optionales Modul**.

Wiederherstellungs-Auftrag: Mit dieser Funktion lassen sich auf Clients oder Gruppen zentral Backups zurückspielen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Wiederherstellungsaufträge im Kapitel **Wiederherstellungsaufträge**. Die Wiederherstellungsfunktion ist verfügbar als Teil des **optionalen Backup-Moduls**.

Softwareerkennungsauftrag: Mit dieser Funktion lässt sich auf Clients installierte Software ermitteln. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareerkennungs-Aufträge im Kapitel **Softwareerkennungsaufträge**. Die Softwareerkennung steht Ihnen zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** verwenden.

Softwareverteilungsauftrag: Mit dieser Funktion lässt sich Software auf Clients verteilen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareverteilungs-Aufträge im Kapitel **Softwareverteilungsaufträge**. Die Softwareverteilung steht Ihnen zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** verwenden.

Sofort (erneut) ausführen: Wählen Sie diese Funktion, um einmalige Scanaufträge, die bereits durchgeführt oder abgebrochen wurden, erneut auszuführen. Bei periodischen Scanaufträgen bewirkt diese Funktion, dass sie unabhängig vom Zeitplan sofort ausgeführt werden.

Protokolle: Rufen Sie mit dieser Funktion die Protokolle zu den Aufträgen des jeweiligen Clients auf.

Alle Aufträge

Nur Scan-Aufträge

Nur Backup-Aufträge (**optionales Backup-Modul**)

Nur Wiederherstellungsaufträge (**optionales Backup-Modul**)

Nur Softwareerkennungsaufträge (**optionales PatchManagement-Modul**)

Nur Softwareverteilungsaufträge (**optionales PatchManagement-Modul**)

Nur Rollback-Aufträge (**optionales PatchManagement-Modul**)

Nur einmalige Scan-Aufträge

Nur periodische Scan-Aufträge

Nur offene Scan-Aufträge

Nur erledigte Scan-Aufträge

Gruppen-Aufträge ausführlich anzeigen: Zeigt bei Gruppenjobs alle zugehörigen Einträge an. Die Option ist nur verfügbar, wenn in der Computerliste eine Gruppe selektiert ist.

In der Menüleiste steht Ihnen für den Aufgabenbereich Aufträge ein zusätzlicher Menüeintrag mit folgenden Funktionen zur Verfügung:

- **Ansicht**: Wählen Sie hier aus, ob Sie sich alle Aufträge anzeigen lassen möchten oder nur spezielle Vorgänge (siehe oben).

- **Sofort (erneut) ausführen**: Hiermit können Sie ausgewählte Jobs unabhängig von eingestellten zeitlichen Vorgaben direkt ausführen.
- **Abbrechen**: Über diese Funktion können Sie einen laufenden Job abbrechen.
- **Löschen**: Ausgewählte Jobs können mit dieser Funktion gelöscht werden.
- **Backup wiederherstellen**: Hiermit können Sie übers Netzwerk Backups auf den Clients einspielen.
- **Neu**: Hier können Sie Vorgänge planen (siehe oben).

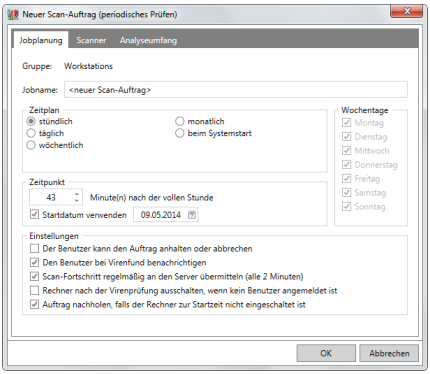
4.4.6.1. Scanaufträge

Im **Neuer Scan-Auftrag**-Fenster können Administratoren einmalige oder regelmäßig wiederkehrende Scan-Aufträge definieren. Eine komplette Job-Konfiguration besteht aus drei Bereichen: **Jobplanung**, **Scanner**-Einstellungen und **Analyseumfang**, jede von diesen ist durch einen eigenen Karteireiter gezielt einstellbar.

Welche Funktionen auf den Registerkarten verfügbar sind, ist abhängig vom ausgewählten Client. Zum Beispiel: Funktionen, die mit Desktop-spezifischen Bedrohungen zu tun haben, sind, wenn Sie einen Auftrag für einen Exchange-Server planen, nicht verfügbar.

Jobplanung

Hier kann festgelegt werden, welchen **Jobnamen** der Scanauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Archivprüfung* oder *Monatliche Prüfung* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Über die Option **Scan-Fortschritt regelmäßig an den Server übermitteln (alle 2 Minuten)** können Sie sich im G Data Administrator den Fortschritt eines laufenden Scanauftrags auf einem Client in Prozent anzeigen lassen.



Darüber hinaus können den Anwendern Berechtigungen zum Anhalten oder Abbrechen des Jobs über das Kontextmenü des Trays eingeräumt werden. Mit der Funktion **Rechner nach der Virenprüfung ausschalten, wenn kein Benutzer**

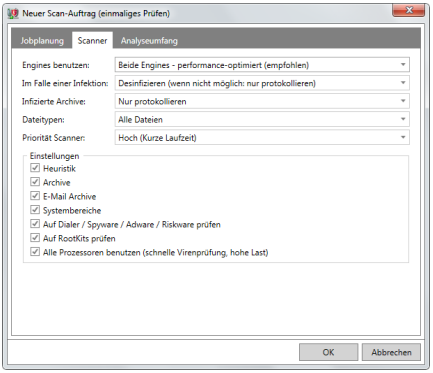
angemeldet ist haben Sie eine weitere Option, die Ihnen hilft, den administrativen Aufwand zu verringern. Sollte ein Rechner zum festgelegten Zeitpunkt eines Scanauftrags nicht eingeschaltet sein, kann über die Option **Auftrag nachholen, falls der Rechner zur Startzeit nicht eingeschaltet ist**, der Scanauftrag gestartet werden, wenn der Rechner nach diesem Zeitpunkt hochgefahren wird.

Bei einmaligen Scanaufträgen können Sie eine Startzeit definieren, bei periodischen Scanaufträgen können Sie festlegen, wann und in welchem Rhythmus die Virenprüfung erfolgen soll. Wird **Beim Systemstart** ausgewählt, fallen die Vorgaben der Zeitplanung weg und die G Data Software führt die Prüfung aus, wenn der Rechner neu gestartet wird. Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Virenprüfung durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

> Wird ein einmaliger Scanauftrag angelegt, steht nur die Option **Startzeit verwenden** zur Verfügung. Ohne Angabe einer Startzeit wird der Scanauftrag sofort nach dem Anlegen gestartet.

Scanner

In dem Scanner-Menü lassen sich die Einstellungen vornehmen, mit denen der Scanauftrag ausgeführt werden soll.



- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenbekämpfung. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. Wir empfehlen die Einstellung **Beide Engines - performance-optimiert**. Hierbei sind beide Virenscanner so miteinander verwoben, dass sie optimale Erkennung mit minimierter Scandauer kombinieren.
- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Diese Einstellungen sind identisch mit denen,

die Sie auf dem Karteireiter **Client-Einstellungen** > **Wächter** vornehmen können.

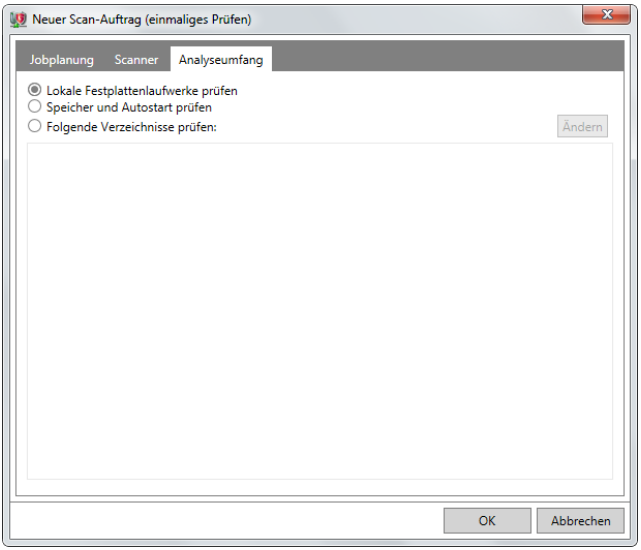
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte Archive behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen**: Hier können Sie festlegen, welche Dateitypen von G Data auf Viren untersucht werden sollen. Beachten Sie, dass eine Überprüfung aller Dateien eines Computers eine gewisse Zeit in Anspruch nehmen kann.
- **Priorität Scanner**: Über die Stufen **Hoch**, **Mittel** und **Niedrig** können Sie festlegen, ob eine Virenprüfung durch G Data auf Ihrem System hohe Priorität haben soll (in diesem Fall erfolgt die Analyse schneller, allerdings sind Performanceeinbußen bei anderen Anwendungen möglich) oder niedrige Priorität (die Analyse benötigt mehr Zeit, dafür werden andere Anwendungen nicht beeinträchtigt). Je nach der Zeit, zu der Sie die Virenanalyse durchführen, sind hier unterschiedliche Einstellungen sinnvoll.
- **Einstellungen**: Legen Sie hier fest, welche zusätzlichen Virenanalysen die G Data Software durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das etwas geringere Maß an Sicherheit aufwiegen. Die meisten Einstellungen sind identisch mit denen, die Sie auf dem Karteireiter **Client-Einstellungen** > **Wächter** finden. Darüber hinaus gibt es aber auch Einstellungen, die speziell für Scanaufträge Verwendung finden:
  - **Auf RootKits prüfen**: Ein Rootkit versucht, sich herkömmlichen Virenerkennungsmethoden zu entziehen. Sie können mit dieser Funktion gezielt nach Rootkits suchen, ohne eine komplette Überprüfung der Festplatten und gespeicherten Daten vorzunehmen.
  - **Alle Prozessoren benutzen**: Mit dieser Option können Sie die Virenprüfung bei Systemen mit mehreren Prozessorkernen auf alle Prozessoren verteilen und auf diese Weise die Virenprüfung deutlich schneller durchführen. Nachteil dieser Option ist, dass so weniger Rechenleistung für andere Anwendungen verfügbar ist. Diese Option sollte nur dann genutzt werden, wenn der Scanauftrag zu Zeiten durchgeführt werden, zu denen das System nicht regulär genutzt wird (z.B. nachts).

Analyseumfang

Über die Registerkarte Analyseumfang lässt sich der Scan-Auftrag auf bestimmte Verzeichnisse (beim Client-Scan) oder Mailboxen (beim Exchange-Scan) begrenzen. Das Verzeichnisauswahl-Fenster erlaubt Ihnen Ordner auf Ihrem Rechner und im Netzwerk auszuwählen. Auf diese Weise können z.B. Ordner mit selten benötigten Archiven ausgenommen und in einem separaten Scanauftrag geprüft werden.

Besonderheit bei Scanaufträgen auf einem Linux-Fileserver: Bei der

Verzeichnisauswahl werden das Root-Laufwerk (/) und alle Freigaben zurückgeliefert. So können Scanaufträge gezielt auf ausgewählten Freigaben oder beliebig gewählten Verzeichnissen des Dateiservers durchgeführt werden.



4.4.6.2. Backupaufträge

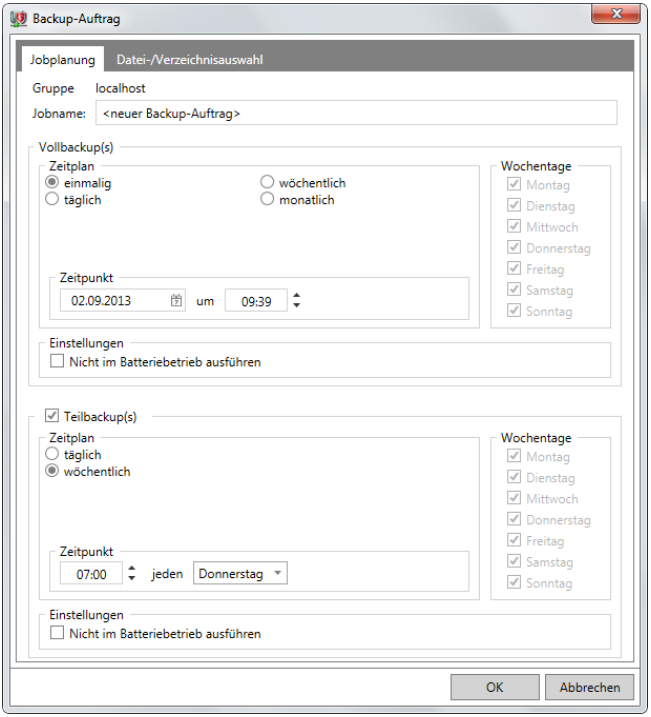
Die Backup-Funktion steht Ihnen als Teil der SmallBusiness Security Software-Version und als optionales Modul zur Verfügung. Hier können Administratoren Backup-Aufträge für Client-Daten initiieren, um wichtige Dateien zentral zu sichern.

Jobplanung

Hier kann festgelegt werden, welchen **Jobnamen** der Backupauftrag haben soll. Hier sollten aussagekräftige Namen, wie z.B. *Monatsbackup* oder *Teilbackup Außendienst* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Sie können hier festlegen, wann und in welchem Rhythmus das Backup erfolgen soll und ob es sich dabei um ein **Teilbackup** oder **Vollbackup** handelt. Beim Teilbackup werden nur die Daten gebackupt, die sich seit dem letzten Teil- oder Vollbackup geändert haben. Dies spart Zeit bei der Erstellung des Backups. Die Wiederherstellung ist im Fall eines Zurückspielens von Daten allerdings langwieriger, da aus den verschiedenen Teilbackupdatenbeständen das letzte Systemabbild rekonstruiert werden muss.

Um Probleme zu vermeiden, die sich beim Abschalten eines nicht ans Stromnetz angeschlossenen Notebooks ergeben, können Sie die Einstellung **Nicht im Batteriebetrieb ausführen** auswählen. Backups von mobilen Geräten erfolgen dann nur, wenn diese auch ans Stromnetz angeschlossen sind. Unter **Täglich** können Sie mit

Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen ein Backup durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.



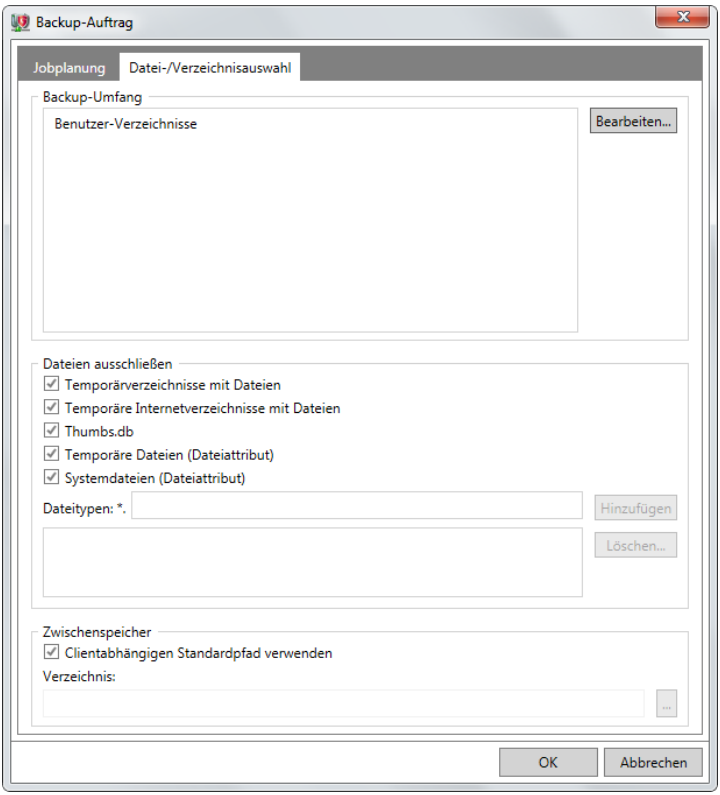
Serverseitige Backupverzeichnisse sowie Warnberichte über Backupspeicherplatz können unter **Server-Einstellungen** > **Backup** konfiguriert werden.

Datei-/Verzeichnisauswahl

Über die Registerkarte Datei-/Verzeichnisauswahl können Sie festlegen, welche Daten genau bei den einzelnen Clients/Gruppen vom Backup erfasst werden sollen. Im Bereich **Backup-Umfang** können Sie dazu direkt im Verzeichnisbaum des jeweiligen Clients die Ordner festlegen, die gesichert werden sollen. Über die Häkchen unter **Dateien ausschließen** können Sie generell Dateien und Ordner mit bestimmten Attributen (z.B. **Temporäre Dateien**, **Systemdateien**) vom Backup ausschließen. Darüber hinaus können Sie auch individuelle Ausnahmen definieren, indem Sie die Endung bestimmter Dateitypen auf die Ausnahmeliste setzen.

Wenn die erstellte Sicherung in einem bestimmten Verzeichnis gespeichert werden soll, bevor Sie an den ManagementServer übermittelt wird, können Sie dies unter **Zwischenspeicher** explizit angeben. Wenn die Option **Clientabhängigen Standardpfad verwenden** nicht aktiv ist und ein absoluter Pfad angegeben ist, wird die Sicherung in dem angegebenen Verzeichnis zwischengespeichert. Wenn Sie die

Option auswählen, wird der G Data Client das Backup immer auf der Partition durchführen, auf der der meiste freie Speicherplatz vorhanden ist. Das Verzeichnis G Data\Backup wird dann im Root-Verzeichnis dieser Partition angelegt.

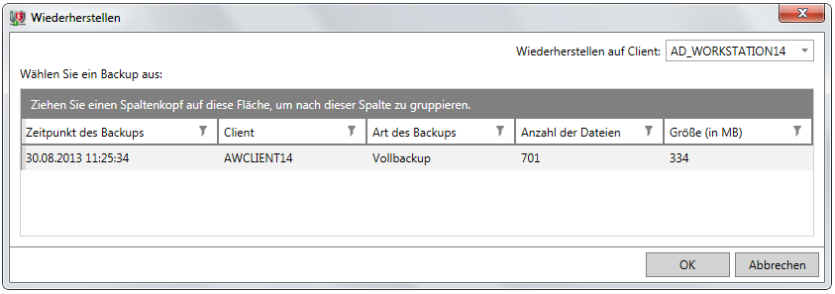


4.4.6.3. Wiederherstellungsaufträge

Wiederherstellungsaufträge können auf unterschiedliche Weise geplant werden. Klicken Sie im Menu **Aufträge** auf **Neu** > **Wiederherstellungsauftrag** oder in der Symbolleiste auf die Schaltfläche **Wiederherstellungsauftrag**. Das Fenster **Backup wiederherstellen** öffnet sich und Sie können ein Backup zum Wiederherstellen auswählen. Alternativ können Sie das Backup in der Auftragsliste suchen. Klicken Sie mit der rechten Maustaste auf den Auftrag und wählen Sie **Backup wiederherstellen**.

Das Fenster Backup wiederherstellen zeigt einige grundlegende Informationen über den ausgewählten Backup-Auftrag. Es enthält ein oder mehrere Backups, je nachdem, wie oft der Auftrag ausgeführt wurde. Die Liste zeigt pro Backup den **Zeitpunkt des Backups**, den **Client**, die **Art des Backups**, die **Anzahl der Dateien** und die **Größe (in MB)**. In der Liste **Wiederherstellen auf Client** können Sie den Client wählen, auf dem die Dateien wiederhergestellt werden sollen (dies muss nicht unbedingt der Client sein, auf dem das Backup erstellt wurde). Klicken Sie auf **OK**, um das Fenster

Wiederherstellungseinstellungen zu öffnen.



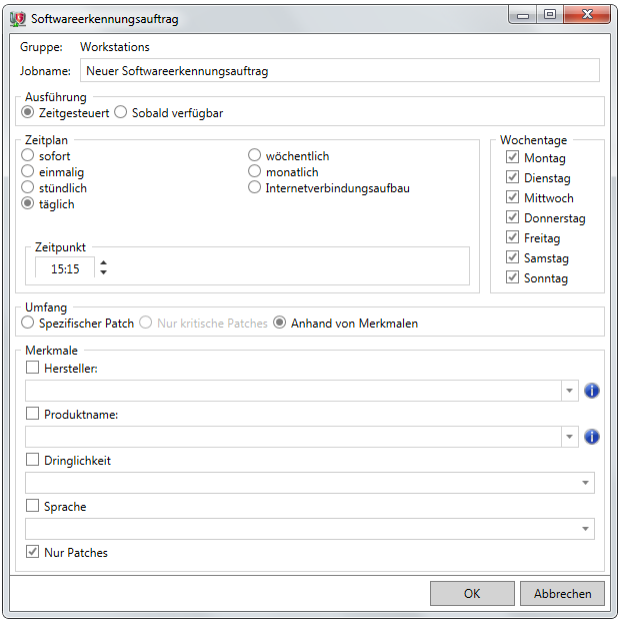
Die Einstellungen für die Wiederherstellung können auf zwei Registerkarten konfiguriert werden. **Auswahl Dateien** ermöglicht es Ihnen, das Backup zu durchsuchen. Klicken Sie auf **Nur ausgewählte Dateien des Archivs wiederherstellen**, um eine Ordnerstruktur zu aktivieren, in der Sie die Dateien, die wiederhergestellt werden sollen, auswählen können. Klicken Sie auf **Alle Dateien des Archivs wiederherstellen**, um die Ordnerstruktur zu deaktivieren und alle Dateien wiederherzustellen. Auf der Registerkarte **Optionen** können Sie die Job-Einstellungen konfigurieren. Sie können unter **Jobname** einen aussagekräftigen Titel eingeben. Wenn Sie die Dateien in ihren ursprünglichen Verzeichnissen wiederherstellen möchten, aktivieren Sie **Dateien in ursprüngliche Verzeichnisse wiederherstellen**. Alternativ wählen Sie ein anderes **Zielverzeichnis**. Schließlich können Sie entscheiden was passieren soll, wenn es Versionskonflikte mit bestehenden Dateien gibt. Nach Bestätigung der Einstellungen wird ein Wiederherstellungsauftrag im Aufträge-Modul hinzugefügt und sofort durchgeführt.

4.4.6.4. Softwareerkennungsaufträge

Die Softwareerkennung steht Ihnen nur zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** installiert haben.

Mit dieser Funktion lässt sich auf Clients oder Gruppen die Anwendbarkeit von verfügbaren **Patches** ermitteln. Die Ausführung der Softwareerkennung kann dabei **Zeitgesteuert** oder **Sobald verfügbar** (jedes Mal, wenn ein neuer Patch verfügbar ist) erfolgen. Zeitgesteuerte Jobs können **Sofort**, **Einmalig** oder nach einem bestimmten Zeitplan ausgeführt werden.

Wählen Sie den **Umfang** der Suche aus. Sie können die Anwendbarkeit **Spezifischer Patches** gezielt prüfen, in dem Sie einen oder mehrere Patches auswählen. Alternativ können Sie die Anwendbarkeit von Software-Patches **Anhand von Merkmalen** ermitteln. Um bestimmte Merkmale (**Hersteller**, **Produktname**, **Dringlichkeit**, **Sprache**) als Auswahlkriterium zuzulassen, setzen Sie bitte das Häkchen beim jeweiligen Merkmal. So können Sie z.B. Software nur von bestimmten Herstellern ermitteln oder konkrete Programmversionen einer Software. Wildcards wie *?* und *** zur Filterung sind dabei zulässig. Wählen Sie **Nur Patches** falls die Softwareerkennung keine vollständigen Software-Pakete und Upgrades auf Anwendbarkeit prüfen soll.



Falls Sie den Softwareerkennungsauftrag über die **Status-Übersicht** des PatchManagers planen, gilt der Auftrag für den Patch und die Client(s), die dort gewählt wurden. Falls Sie den Auftrag über das **Patch-Konfiguration**-Modul planen, wählen Sie im Auftragsfenster die Clients, für die die Anwendbarkeit geprüft werden soll. Falls Sie den Auftrag über das **Aufträge**-Modul planen, wählen Sie im Auftragsfenster die Patches, deren Anwendbarkeit geprüft werden soll - der Job wird auf dem aktuell ausgewählten Client oder der aktuell ausgewählten Gruppe ausgeführt.

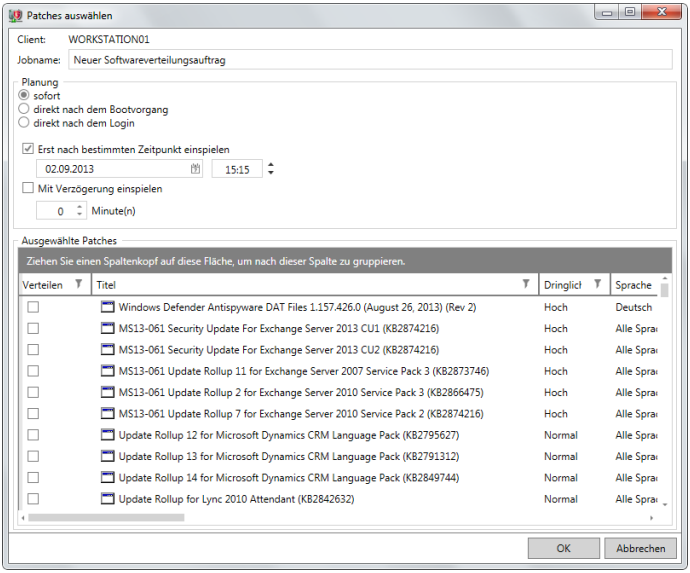
4.4.6.5. Softwareverteilungsaufträge

Die Softwareverteilung steht Ihnen nur zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** installiert haben.

Um **anwendbare Patches** auf Clients und Gruppen zu installieren, definieren Sie einen Softwareverteilungsauftrag. Durch Auswahl der Option **Erst nach bestimmten Zeitpunkt einspielen** können Sie den Job zeitlich planen. Wählen Sie unter **Ausgewählte Patches** einen oder mehrere Patches. Die Softwareverteilung kann **Sofort**, **Direkt nach dem Bootvorgang**, oder **Direkt nach dem Login** stattfinden. Über die Einstellung bei **Mit Verzögerung einspielen** können Sie das Einspielen von Patches zeitlich vom Bootvorgang trennen. Vorteil hierbei: Bootvorgang und Patcheinspielung beeinträchtigen nicht beide gleichzeitig die Performance des Clients.

Falls Sie den Softwareverteilungsauftrag über die **Status-Übersicht** des PatchManagers planen, gilt der Auftrag für den Patch und die Client(s), die dort gewählt wurden. Falls Sie den Auftrag über das **Patch-Konfiguration**-Modul planen, wählen Sie im Auftragsfenster die Clients, auf denen der Patch installiert werden soll. Falls Sie

den Auftrag über das **Aufträge**-Modul planen, wählen Sie im Auftragsfenster die Patches, die installiert werden sollen - der Job wird auf dem aktuell ausgewählten Client oder der aktuell ausgewählten Gruppe ausgeführt.


Patches auswählen
Client: WORKSTATION01
Jobname: Neuer Softwareverteilungsauftrag
Planung
sofort
direkt nach dem Bootvorgang
direkt nach dem Login
Erst nach bestimmten Zeitpunkt einspielen
02.09.2013
15:15
Mit Verzögerung einspielen
0
Minute(n)
Ausgewählte Patches
Ziehen Sie einen Spaltenkopf auf diese Fläche, um nach dieser Spalte zu gruppieren.
Verteilen
Titel
Dringlicl
Sprache
Windows Defender Antispyware DAT Files 1.157.426.0 (August 26, 2013) (Rev 2) Hoch Deutsch
MS13-061 Security Update For Exchange Server 2013 CU1 (KB2874216) Hoch Alle Spra
MS13-061 Security Update For Exchange Server 2013 CU2 (KB2874216) Hoch Alle Spra
MS13-061 Update Rollup 11 for Exchange Server 2007 Service Pack 3 (KB2873746) Hoch Alle Spra
MS13-061 Update Rollup 2 for Exchange Server 2010 Service Pack 3 (KB2866475) Hoch Alle Spra
MS13-061 Update Rollup 7 for Exchange Server 2010 Service Pack 2 (KB2874216) Hoch Alle Spra
Update Rollup 12 for Microsoft Dynamics CRM Language Pack (KB2795627) Normal Alle Spra
Update Rollup 13 for Microsoft Dynamics CRM Language Pack (KB2791312) Normal Alle Spra
Update Rollup 14 for Microsoft Dynamics CRM Language Pack (KB2849744) Normal Alle Spra
Update Rollup for Lync 2010 Attendant (KB2842632) Normal Alle Spra
OK
Abbrechen

4.4.6.6. Rollbackauftrag

Der Rollbackauftrag steht Ihnen nur zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** installiert haben.

Um bereits eingespielte Patches zu deinstallieren, können Sie einen Rollback-Vorgang über die **Status-Übersicht** des PatchManagers durchführen oder direkt per Rechtsklick in der Aufgabenliste auf den jeweiligen Distributionsjob durch Auswahl der Funktion **Rollback**.

4.4.7. PolicyManager

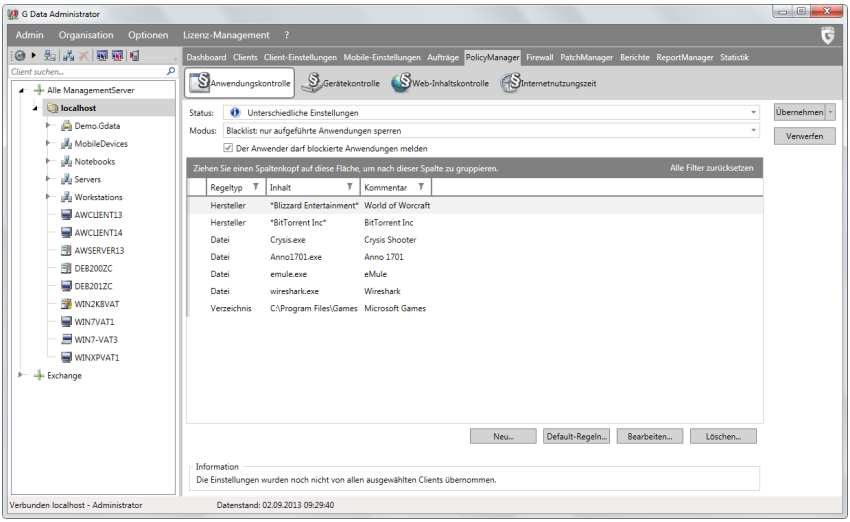
Das Modul PolicyManager steht Ihnen nur als Teil der Software-Version EndpointProtection zur **Verfügung**.

Der PolicyManager enthält eine Anwendungs-, Geräte-, Web-Inhaltskontrolle sowie eine Überwachung der Internetnutzungszeit. Diese Funktionen erlauben eine flächendeckende Umsetzung der Unternehmensrichtlinien zur Nutzung der firmeneigenen PCs. So kann über den PolicyManager bestimmt werden, ob und in welchem Umfang externe Massenspeicher- oder optische Medien genutzt werden können. Ebenso lässt sich definieren, welche Webseiten besucht und welche Programme auf den Firmen-PCs genutzt werden dürfen.

4.4.7.1. Anwendungskontrolle

Mit der Anwendungskontrolle lassen sich bestimmte Programme für die Nutzung durch ausgewählte Clients sperren. Legen Sie dazu unter **Status** fest, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Unter Modus bestimmen Sie nun, ob es sich bei der Anwendungskontrollliste um eine Whitelist oder Blacklist handeln soll.

- **Whitelist**: Nur die hier aufgeführten Anwendungen können vom Client-Rechner aus verwendet werden.
- **Blacklist**: Hier aufgeführte Anwendungen können auf dem Client-Rechner nicht verwendet werden.



Über die **Neu**-Schaltfläche, kann eine neue Regel erstellt werden. Zur Auswahl stehen die Regeltypen **Hersteller**, **Datei** und **Verzeichnis**:

- **Hersteller**: Hier werden die Herstellerinformationen in Programmdateien dazu verwendet, eine Nutzung dieser Anwendungen zu erlauben oder zu verbieten. Sie können den Namen des Herstellers hier entweder selbst eintragen oder über die **...**-Schaltfläche gezielt eine Datei auswählen, aus der die Herstellerinformation ausgelesen und übernommen wird.
- **Datei**: Hier können Sie bestimmte Programmdateien für den jeweiligen Client sperren oder erlauben. Dabei können Sie entweder den Dateinamen eingeben, um den Zugriff auf Dateien dieses Namens generell zu verbieten/zu erlauben oder Sie klicken auf die Schaltfläche **Merkmale einer Datei ermitteln**, um ganz speziell eine bestimmte Datei anhand ihrer Merkmale zu definieren. Bei Bedarf können Sie als Platzhalter für beliebige Inhalte einen Stern (*) am Anfang und/oder Ende der Merkmale **Dateiname**, **Produktname** und **Copyright**

verwenden.

- **Verzeichnis**: Über diese Funktion können Sie komplette Verzeichnisse (auf Wunsch inklusive der jeweiligen Unterverzeichnisse) für Clients freigeben oder sperren.

4.4.7.2. Gerätekontrolle

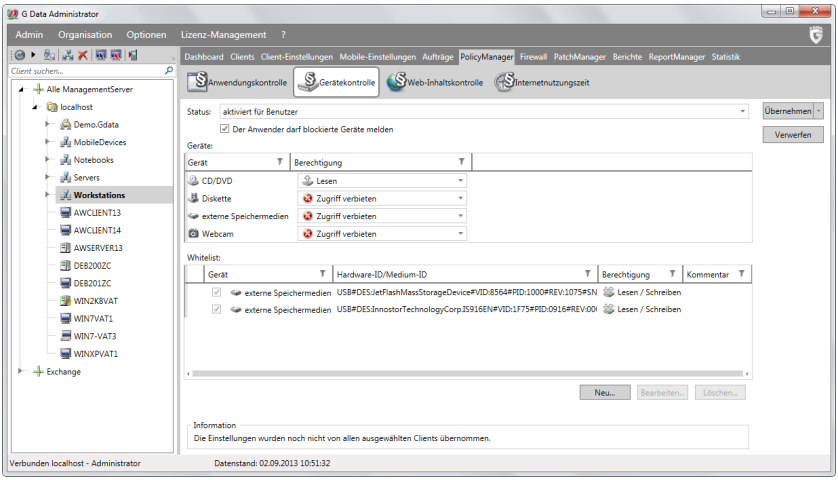
Mit Hilfe der Gerätekontrolle lässt sich der Zugriff auf externe Speichermedien begrenzen. So können USB-Sticks von der Nutzung ausgeschlossen, CD/DVD-Laufwerke mit Schreib- oder Leserechten ausgestattet und auch die Verwendung von Kameras eingeschränkt werden.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Für jeden Client werden unter **Geräte** die Geräteklassen angezeigt, deren Nutzung eingeschränkt werden kann. Diese müssen nicht zwangsläufig auch am jeweiligen Client vorhanden sein. So kann zum Beispiel für ausgewählte Nutzergruppen generell die Nutzung von Diskettenlaufwerken untersagt werden, unabhängig davon, ob die jeweiligen Rechner ein Diskettenlaufwerk besitzen oder nicht. Folgende Berechtigungen lassen sich definieren:

Lesen / Schreiben: Es besteht voller Zugriff auf das Gerät.

Lesen: Medien können nur gelesen werden, ein Abspeichern von Daten ist nicht erlaubt.

Zugriff verbieten: Sowohl Lese- als auch Schreibzugriffe auf das Gerät sind nicht erlaubt. Das Gerät kann vom Anwender nicht verwendet werden.



Über die **Whitelist**-Einstellungen können Sie die Gerätenutzung, die Sie für den Client-Nutzer in irgendeiner Weise eingeschränkt haben (**Lesen / Zugriff verbieten**) mit bestimmten Einschränkungen wieder erlauben. Wenn Sie auf die **Neu**-Schaltfläche klicken, öffnet sich ein Dialogfenster, in dem die Geräte mit Nutzungseinschränkungen angezeigt werden. Wenn Sie nun auf **...** klicken, können Sie für bestimmte Geräte eine Ausnahme zulassen.

- **Medium-ID verwenden**: Hier können Sie z.B. festlegen, dass nur bestimmte CDs oder DVDs mit einem CD/DVD-Laufwerk genutzt werden können (z.B. spezielle Firmen-Präsentationen auf CD).
- **Hardware-ID verwenden**: Hier können Sie z.B. festlegen, dass nur bestimmte USB-Sticks verwendet werden dürfen. Bei Hardware-ID-basierten Freigaben für einzelne Speichergeräte hat der Netzwerkadministrator die Möglichkeit, zu kontrollieren, welche Mitarbeiter die Möglichkeit zur Weitergabe von Daten haben.

Um eine Medium-ID oder Hardware-ID zu ermitteln, klicken Sie auf den Eintrag **Quelle auswählen** und wählen dort den Client aus, auf dem sich das freizugebende Medium befindet. Die entsprechende ID wird dann automatisch ausgelesen. Über die lokale Suche können Sie die ID des Mediums oder der Hardware mit Hilfe des Rechners ermitteln, auf dem der G Data Administrator installiert ist. Das Medium muss dazu an die entsprechende Maschine angeschlossen bzw. dort eingelegt sein.

4.4.7.3. Web-Inhaltskontrolle

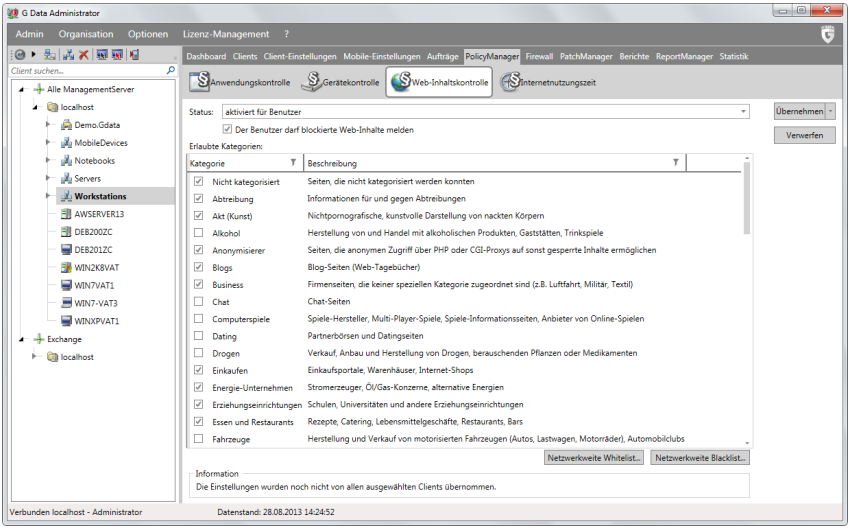
Die Web-Inhaltskontrolle dient dazu, Anwendern zwar den dienstlichen Zugang zum Internet zu erlauben, aber das Surfen auf nicht erwünschten Websites oder in bestimmten Themenbereichen zu unterbinden. Sie können hier gezielt Bereiche durch Setzen eines Häkchens für den jeweiligen Client erlauben oder durch Entfernen des Häkchens verbieten. Die Kategorien decken dabei eine große Anzahl thematischer Bereiche ab und werden von G Data laufend aktualisiert. Somit entfällt für den Netzwerkadministrator der mit der Pflege von White- und Blacklists verbundene Aufwand.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorenrechte auf dem Client-Rechner besitzen.

Mit der **Netzwerkweiten Whitelist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten unternehmensweit für das gesamte Netzwerk freigegeben werden. Dies kann z.B. die Webpräsenz Ihres Unternehmens sein. Geben Sie dazu unter **URLs** die Adresse ein, die freigegeben werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechende Seite ist freigegeben.

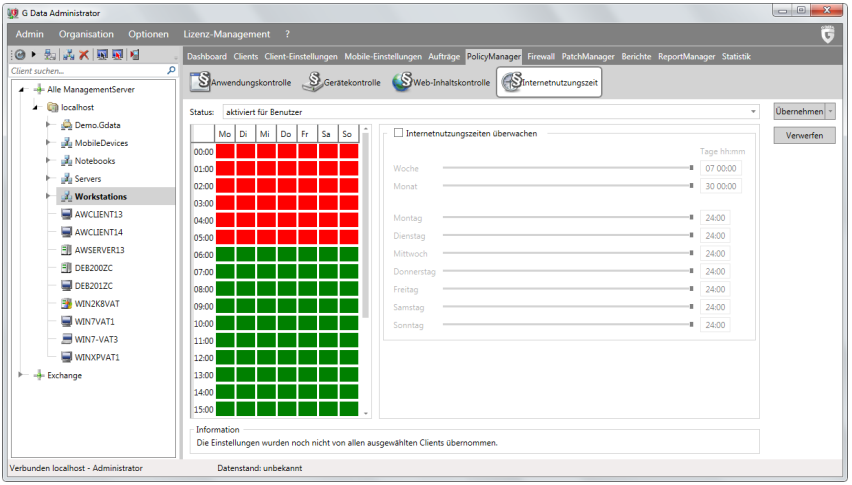
Mit der **Netzwerkweiten Blacklist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten

unternehmensweit für das gesamte Netzwerk gesperrt werden. Geben Sie dazu unter **URLs** die Adresse ein, die gesperrt werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechende Seite ist gesperrt.



4.4.7.4. Internetnutzungszeit

Im Bereich Internetnutzungszeit kann die generelle Nutzung des Internets auf bestimmte Zeiten beschränkt werden. Zudem ist auch die Einrichtung eines Zeitkontingents für die Internetnutzung möglich. Unter **Status** wird festgelegt, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen.



Auf der rechten Seite kann über die dort vorhandenen Schieberegler das Kontingent festgelegt werden, dass auf dem jeweiligen Clientrechner für die Nutzung des Internets zur Verfügung steht. Es können tägliche, wöchentliche oder monatliche Kontingente vergeben werden; beispielsweise entspricht die Angabe *04 20:05* einer Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten. Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat.

> Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.

Im Sperrzeiten-Bereich können Sie - zusätzlich zur zeitlichen Eingrenzung der Internetnutzung - bestimmte Zeiträume sperren. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen Zeitraum freizugeben oder zu sperren, markieren Sie diesen mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben: **Zeit freigeben** und **Zeit sperren**. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.

4.4.8. Firewall

Das Firewall-Modul steht Ihnen nur in den Software-Versionen ClientSecurity und EndpointProtection zur **Verfügung**.

In diesem Bereich kann die Firewall auf den jeweiligen Clients oder Gruppen zentral administriert werden. **Übersicht** bietet dem Systemadministrator eine Übersicht über den aktuellen Status der Firewall auf den installierten Clients, **Regelsätze** bietet Möglichkeiten zum Erstellen und Verwalten von Regelsätzen.

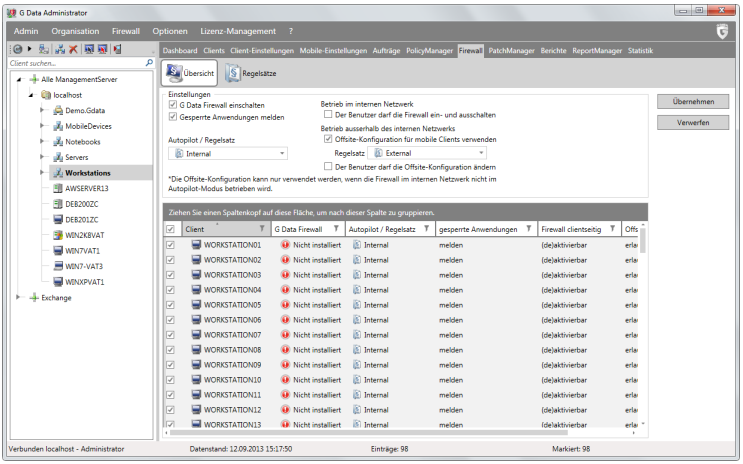
4.4.8.1. Übersicht

Es gibt zwei grundsätzlich verschiedene Möglichkeiten, eine Firewall zu betreiben. Wenn die Firewall auf **Autopilot** betrieben wird, ist sie schon standardmäßig von G Data vorkonfiguriert, erfüllt Ihre Aufgabe im Hintergrund und stört den Anwender nicht mit Rückfragen. Im Autopilotmodus optimiert die Firewall ihren Regelsatz mit der Zeit selbstständig. Als Administrator können Sie auch individuelle Firewallregeln für unterschiedliche Netzwerkbereiche definieren (**Regelsätze**).

Einige allgemeine Firewall-Einstellungen können hier konfiguriert werden:

- **G Data Firewall einschalten**: Durch Setzen des Häkchens wird die Firewall auf dem jeweiligen Client aktiviert. Wenn Sie das Häkchen entfernen, ist die Firewall inaktiv.

- **Gesperrte Anwendungen melden**: Wenn dieses Häkchen gesetzt ist und der Client-Rechner mit dem G Data ManagementServer verbunden ist, erhält der Systemadministrator im Bereich **Berichte** Informationen über Anwendungen, die durch die jeweilige Client-Firewall geblockt wurden.
- **Der Benutzer darf die Firewall ein- und ausschalten**: Hier können Sie als Netzwerkadministrator dem Nutzer des Client-Rechners erlauben, die Firewall zwischenzeitlich auszuschalten. Diese Möglichkeit ist nur dann gegeben, solange sich der Client innerhalb des Firmennetzwerks befindet und sollte natürlich nur versierten Anwendern ermöglicht werden.
- **Offsite-Konfiguration für mobile Clients verwenden**: In der Offsite-Konfiguration werden die Firewall-Regelsätze des Client-Rechners, die in Ihrem Firmennetzwerk gelten, durch Standardregelsätze ersetzt, die automatisch den Umgang mit dem Internet, sicheren-, unsicheren und zu blockierenden Netzen regeln. Auf diese Weise ist der mobile Rechner optimal geschützt, solange er sich nicht im Netzwerk des G Data ManagementServers befindet. Sobald der mobile Rechner wieder mit dem Netzwerk des G Data MangementServers verbunden wird, werden diese Standardregelsätze automatisch wieder durch die Regelsätze ersetzt, wie sie für den jeweiligen Client in Ihrem Netzwerk gelten.
- **Der Benutzer darf die Offsite-Konfiguration ändern**: Diese Option soll es versierten Anwendern erlauben, ihre Firewall außerhalb des Netzwerks individuell zu konfigurieren. Sobald der mobile Rechner wieder mit dem G Data ManagementServer verbunden wird, werden die durchgeführten Änderungen wieder durch die vom Netzwerkadministrator vorgegebenen Regeln für diesen Client ersetzt. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird. Wenn der jeweilige Client im Firmennetzwerk die Autopilot-Einstellungen für die Firewall verwendet, werden die Autopilot-Einstellungen auch dann verwendet, wenn der Client nicht mit dem Netzwerk verbunden ist.



In der Übersicht werden alle Client-Rechner oder die Clients einer ausgewählten Gruppe angezeigt. Hier sehen Sie auf einen Blick, welche Einstellungen die jeweilige Client-Firewall hat und können durch Anklicken des jeweiligen Clients direkt Änderungen vornehmen. Folgende Informationen hält die Übersichtsliste bereit:

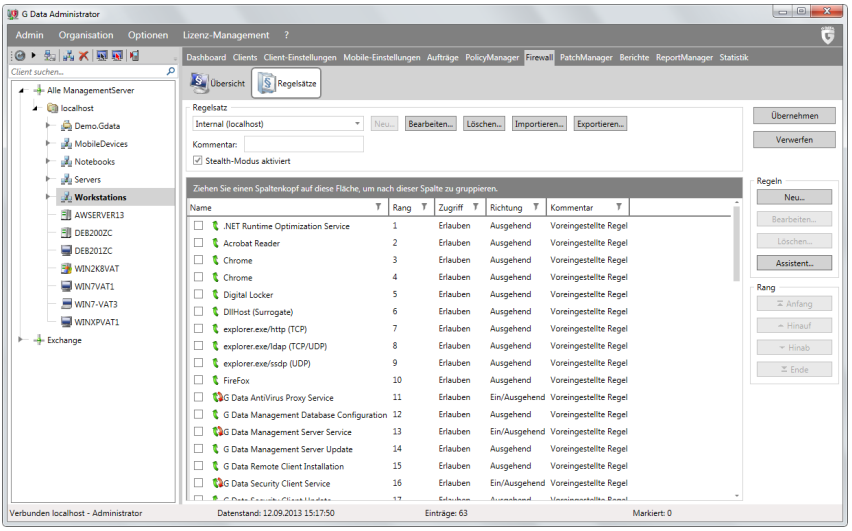
- **Client**: Der Name des Client-Rechners. Anhand des abgebildeten Symbols können Sie hier erkennen, ob die Client-Software auf diesem Client installiert ist.
- **G Data Firewall**: Hier erfahren Sie, ob die Firewall auf dem Client eingeschaltet, ausgeschaltet oder ggf. gar nicht installiert ist.
- **Autopilot / Regelsatz**: Zeigt an, welcher Regelsatz für welchen Client angewendet wird.
- **Gesperrte Anwendungen**: Zeigt, ob blockierte Anwendungen bei Nutzungsaufruf gemeldet werden oder nicht.
- **Firewall clientseitig**: Hier sehen Sie, ob der Client-Benutzer die Firewall aktivieren bzw. deaktivieren kann.
- **Offsite-Konfiguration**: Wenn Sie für einen Client die Offsite-Konfiguration auswählen, kann der Anwender auf diesem Client seine Firewall-Einstellungen individuell verwalten und einstellen, solange er nicht mit dem Netzwerk des G Data ManagementServers verbunden ist. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird.

Um die Firewall-Einstellungen für die in der Liste ausgewählten Clients zu ändern, klicken Sie den Eintrag mit der rechten Maustaste an. Es öffnet sich ein Auswahlmenü mit folgenden Optionen:

- **Regelsatz erstellen**: Hiermit wechseln Sie in den Bereich **Regelsätze** und können individuelle Regeln für ihre Client-Firewalls definieren.
- **Regelsatz bearbeiten**: Hiermit wechseln Sie in den Bereich **Regelsätze** und können bestehende Regeln für ihre Client-Firewalls ändern.
- **G Data Firewall installieren**: Starten Sie eine Remote-Installation der G Data Firewall. Dazu müssen die Systemanforderungen für eine Remote-Installation erfüllt sein (siehe **G Data Security Client Remote-Installation**).
- **G Data Firewall deinstallieren**: Mit dieser Funktion wird die bestehende Client-Firewall deinstalliert.

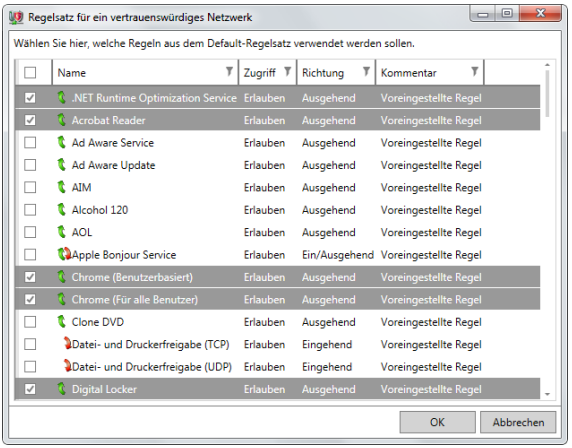
4.4.8.2. Regelsätze

Auf der Registerkarte Regelsätze können Sie Regelsätze für unterschiedliche Netzwerkbereiche erstellen. Jeder Regelsatz kann eine beliebige Anzahl von Firewall-Regeln beinhalten.



Regelsatz erstellen

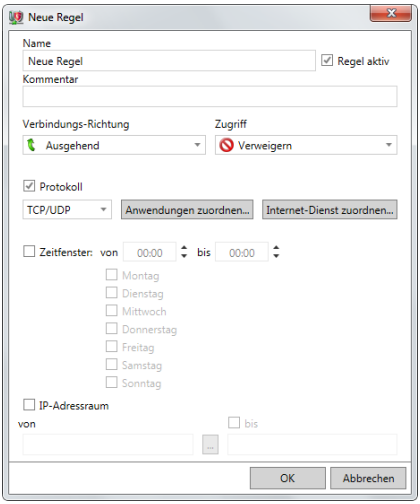
Klicken Sie bei **Regelsatz** auf die Schaltfläche **Neu** um das Fenster **Neuer Regelsatz** zu öffnen. Geben Sie einen **Namen** für den Regelsatz und ggf. **Kommentar** ein. Wählen Sie **Stealth-Modus aktiv** um Anfragen an den Computer, die dazu dienen, die Erreichbarkeit von Ports zu überprüfen, nicht zu beantworten. Dies erschwert es Angreifern, auf diese Weise Informationen über das System zu erhalten. Klicken Sie auf **OK** um das Fenster **Regelsatz für ein vertrauenswürdiges Netzwerk** zu öffnen. Sie haben die Möglichkeit, aus einer großen Anzahl von Default-Regeln und ggf. selbst angelegten Regeln einen individuell auf den Client zugeschnittenen Regelsatz aufzustellen. Nachdem Sie **OK** wählen, wird der Regelsatz in der **Regelsätze**-Übersicht gezeigt. Sie können mit Hilfe der Schaltflächen **Löschen** und **Bearbeiten** bestehende Regelsätze verwalten. Regelsätze können als XML-Datei importiert und exportiert werden.


Regelsatz für ein vertrauenswürdiges Netzwerk
Wählen Sie hier, welche Regeln aus dem Default-Regelsatz verwendet werden sollen.
Name
Zugriff
Richtung
Kommentar
.NET Runtime Optimization Service Erlauben Ausgehend Voreingestellte Regel
Acrobat Reader Erlauben Ausgehend Voreingestellte Regel
Ad Aware Service Erlauben Ausgehend Voreingestellte Regel
Ad Aware Update Erlauben Ausgehend Voreingestellte Regel
AIM Erlauben Ausgehend Voreingestellte Regel
Alcohol 120 Erlauben Ausgehend Voreingestellte Regel
AOL Erlauben Ausgehend Voreingestellte Regel
Apple Bonjour Service Erlauben Ein/Ausgehend Voreingestellte Regel
Chrome (Benutzerbasiert) Erlauben Ausgehend Voreingestellte Regel
Chrome (Für alle Benutzer) Erlauben Ausgehend Voreingestellte Regel
Clone DVD Erlauben Ausgehend Voreingestellte Regel
Datei- und Druckerfreigabe (TCP) Erlauben Eingehend Voreingestellte Regel
Datei- und Druckerfreigabe (UDP) Erlauben Eingehend Voreingestellte Regel
Digital Locker Erlauben Ausgehend Voreingestellte Regel
OK
Abbrechen

Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.

Regel erstellen/Regel bearbeiten

Alle Regeln des aktuellen Regelsatzes sind in der Listenansicht aufgelistet. Verwenden Sie unter **Regeln** die Schaltflächen **Neu** und **Bearbeiten**, um neue Regeln hinzuzufügen oder bestehende zu verändern.

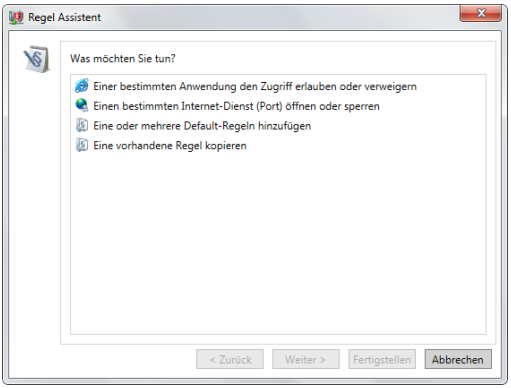


- **Name**: Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programmname für den die jeweilige Regel zutrifft.
- **Regel aktiv**: Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar**: Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht *Voreingestellte Regel*, bei Regeln, die sich aus dem Dialog aus dem Firewall-Alarm ergeben steht *Per Nachfrage generiert* und für Regeln, die Sie selber über den Profi-Dialog generieren, können Sie einen eigenen Kommentar einfügen.
- **Verbindungs-Richtung**: Mit der Richtung wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff**: Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.

- **Protokoll**: Hier können Sie auswählen, welchen Verbindungsprotokollen Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu verbinden (**Anwendungen zuordnen**). Genauso können Sie die unerwünschten bzw. erwünschten Ports über die Schaltfläche **Internet-Dienst zuordnen** genau definieren.
- **Zeitfenster**: Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum**: Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Angriffs deutlich.

Regelassistent

Mit dem Regelassistenten können Sie auf einfache Weise zusätzliche Regeln für den jeweiligen Regelsatz definieren. Mit dem Regelassistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz.


Regel Assistent
Was möchten Sie tun?
Einer bestimmten Anwendung den Zugriff erlauben oder verweigern
Einen bestimmten Internet-Dienst (Port) öffnen oder sperren
Eine oder mehrere Default-Regeln hinzufügen
Eine vorhandene Regel kopieren
< Zurück
Weiter >
Fertigstellen
Abbrechen

Der Regelassistent stellt folgende Aktionen zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern**: Hiermit können Sie gezielt eine Anwendung auswählen und ihr im Rahmen des gewählten Regelsatzes den Zugriff auf das Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (Programmpfad) und geben Sie dann unter **Verbindungs-Richtung** an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).

- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren**: Im Assistenten haben Sie die Möglichkeit, Ports komplett zu sperren oder aber auch nur für eine bestimme Anwendung (z.B. CRM-Software) freizugeben.
- **Eine oder mehrere Default-Regeln hinzufügen**: Mit dieser Funktion können Sie eine oder mehrere Default-Regeln zu dem gewählten Regelsatz hinzufügen.
- **Eine vorhandene Regel kopieren**: Mit dieser Funktion können Sie zum weiteren Editieren eine Kopie einer bestehenden Regel anfertigen.

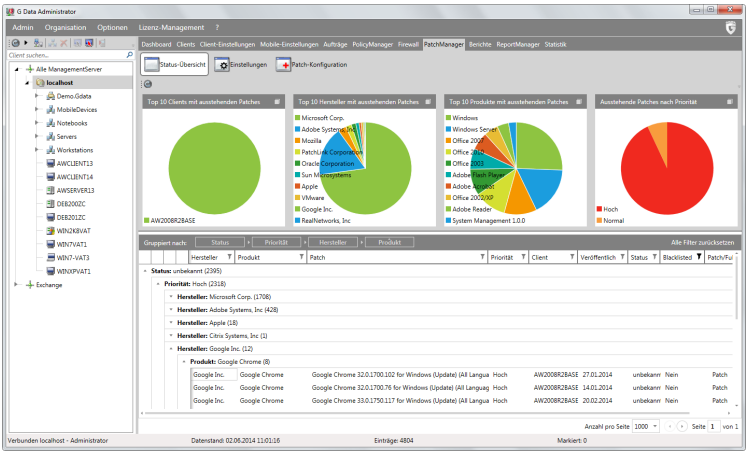
4.4.9. PatchManager

Der PatchManager ist ein optionales Modul für die Nutzer der AntiVirus, ClientSecurity und Endpoint-Protection **Software-Lösungen**.

Mit Hilfe des PatchManagers können Sie die Patch-Implementierung für alle verwalteten Clients über eine einzige Schnittstelle steuern. Sie können den PatchManager sowohl für Updates von Microsoft-Software, als auch anderen Anbietern nutzen. Jeder Patch kann auf Anwendbarkeit überprüft werden, auf eine Blacklist gesetzt werden, distribuiert oder übers Rollback zurückgenommen werden. Dies funktioniert sowohl für einzelne Clients, als auch für Client-Gruppen.

4.4.9.1. Status-Übersicht

Der Status-Übersichtsbereich bietet Ihnen eine detaillierte Übersicht über Patches und deren Status innerhalb des Netzwerks. Der Bereich listet alle Patches in alphabetischer Reihenfolge und einmal für jeden Client auf. Die umfangreiche Liste kann gefiltert werden, um z.B. zu zeigen ob alle Clients mit allen relevanten Patches aktualisiert wurden. Hier können Sie auch direkt die Patch-Bereitstellung planen. Eine Reihe von Grafiken zeigt Informationen über ausstehende Patches, z.B. ob es kritische Patches gibt, die noch installiert werden müssen.



Standardmäßig ist die Status-Übersicht nach **Status**, **Priorität**, **Hersteller** und **Produkt** gruppiert, um schnell feststellen zu können, ob wesentliche Patches schon installiert sind oder nicht. Darüber hinaus sind standardmäßig Filter aktiv, die vollständige Software-Pakete sowie geblacklistete Patches ausblenden. Wählen Sie **Alle Filter zurücksetzen**, um alle Listeneinträge anzeigen zu lassen.

Pro Patch und Client können Sie verschiedene Aufträge planen. Wählen Sie einen oder mehrere Patches mit der rechten Maustaste und klicken Sie eine der folgenden Optionen an:

- **Patches auf Anwendbarkeit prüfen**: Planen Sie mit Hilfe vom **Softwareerkennungs**-Fenster einen Auftrag, der die selektierten Patches auf Anwendbarkeit auf dem selektierten Client prüft.
- **Patches installieren**: Planen Sie mit Hilfe vom **Softwareverteilungs**-Fenster einen Auftrag, der die selektierten Patches auf dem selektierten Client installiert.
- **Rollback**: Planen Sie einen **Rollback**-Job für Patches, die bereits installiert worden sind.
- **Patches auf die Blacklist setzen**: Setzt einen oder mehrere Patches auf die Blacklist.
- **Patches von der Blacklist entfernen**: Entfernt einen oder mehrere Patches von der Blacklist.
- **Eigenschaften**: Zeigt weitere Informationen an, wie z.B. eine komplette Beschreibung und den Lizenztext.

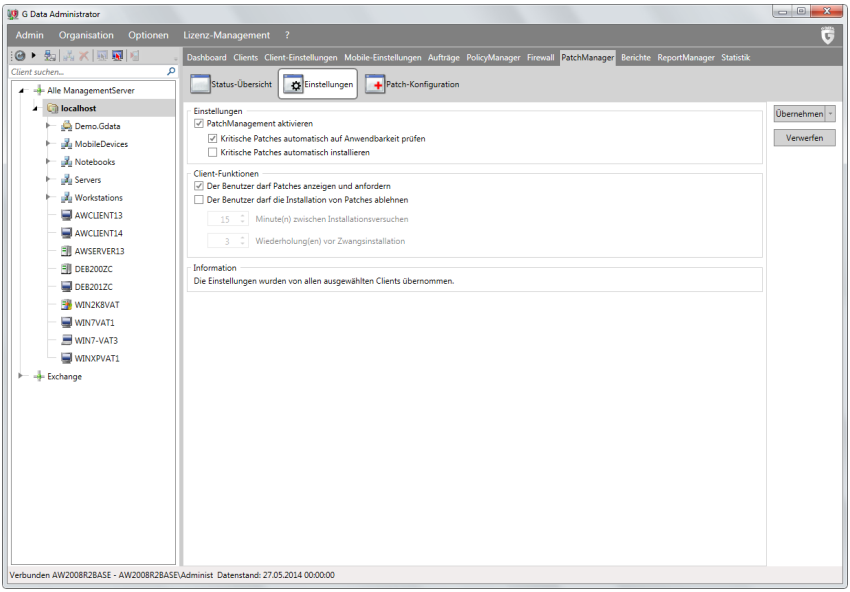
Die **Status**-Spalte zeigt den Status jedes Patches und seine geplanten oder laufenden Patch-Jobs (z.B. *Wird geprüft* während ein Auftrag ausgeführt wird oder *Nicht anwendbar* falls der Patch nicht anwendbar ist).

4.4.9.2. Einstellungen

Hier können Sie bestimmen, wie Patches und Updates auf dem Client und den Gruppen eingespielt werden sollen.

- **PatchManagement aktivieren**: PatchManager ein- oder ausschalten.
  - **Kritische Patches automatisch auf Anwendbarkeit prüfen**: Sobald ein Patch mit kritischer Priorität freigegeben wird, kann PatchManager die Anwendbarkeit automatisch überprüfen. Für kritische Patches brauchen Sie dann keine separaten Patchanwendbarkeitsjobs mehr definieren.
  - **Kritische Patches automatisch installieren**: Sobald ein Patch mit kritischer Priorität freigegeben wird, kann PatchManager den Patch automatisch installieren (falls er anwendbar ist). Dies könnte zu Kompatibilitätsproblemen auf den Clients führen. Die Kompatibilität sollte vorher auf einer Auswahl von Testclients überprüft werden.

- **Der Benutzer darf Patches anzeigen und anfordern**: Der Benutzer darf verfügbare Patches anzeigen und die Bereitstellung anfordern.
- **Der Benutzer darf die Installation von Patches ablehnen**: Der Benutzer darf eine Patch-Installation zumindest zeitweise verweigern. Sie können hierbei festlegen, wie oft der Anwender die Installation ablehnen kann, bis die Installation zwangsweise durchgeführt wird und bestimmen, wie oft eine Patch-Installation vom System versucht werden soll.



4.4.9.3. Patch-Konfiguration

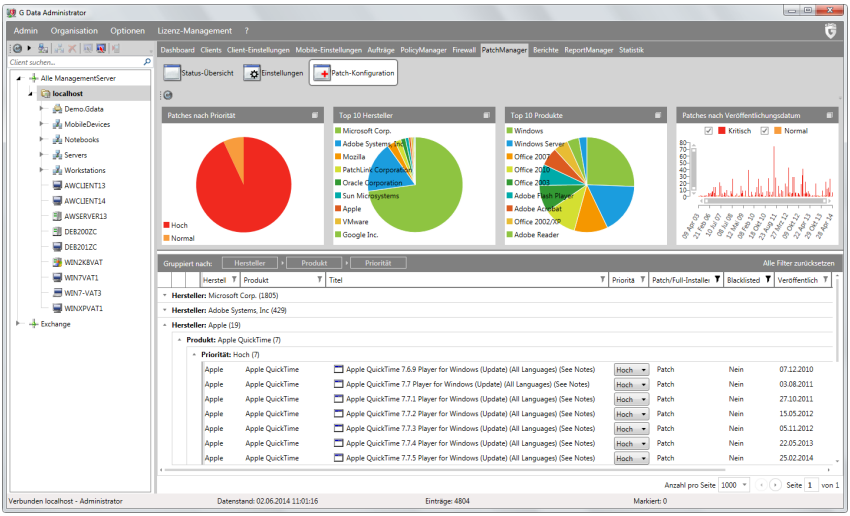
Im Bereich Patch-Konfiguration können Sie alle bekannten systemweiten Patches zentral verwalten. Eine Reihe von Grafiken zeigt Statistiken über Patches, Produkte und Hersteller.

Standardmäßig sind Patches nach **Hersteller**, **Produkt** und **Priorität** gruppiert, so dass Sie schnell Patches für das jeweilige Produkt finden. Darüber hinaus sind standardmäßig Filter aktiv, die vollständige Software-Pakete sowie geblacklistete Patches ausblenden. Wählen Sie **Alle Filter zurücksetzen**, um alle Listeneinträge anzeigen zu lassen.

Pro Patch können Sie verschiedene Aufträge planen. Wählen Sie einen Patch mit der rechten Maustaste und klicken Sie eine der folgenden Optionen an:

- **Patches auf Anwendbarkeit prüfen**: Planen Sie mit Hilfe vom **Softwareerkennungs**-Fenster einen Auftrag, der die selektierten Patches auf Anwendbarkeit auf dem selektierten Client prüft.

- **Patches installieren**: Planen Sie mit Hilfe vom **Softwareverteilungs**-Fenster einen Auftrag, der die selektierten Patches auf dem selektierten Client installiert.
- **Patches auf die Blacklist setzen**: Setzt einen oder mehrere Patches auf die Blacklist.
- **Patches von der Blacklist entfernen**: Entfernt einen oder mehrere Patches von der Blacklist.
- **Eigenschaften**: Zeigt weitere Informationen an, wie z.B. eine komplette Beschreibung und den Lizenztext.



Die **Priorität**-Spalte zeigt die Priorität jedes Patches. Die hier vorgegebenen Standardprioritäten, die auf den Vorgaben der internen PatchManager-Datenbank basieren, können hier auch von Ihnen geändert werden.

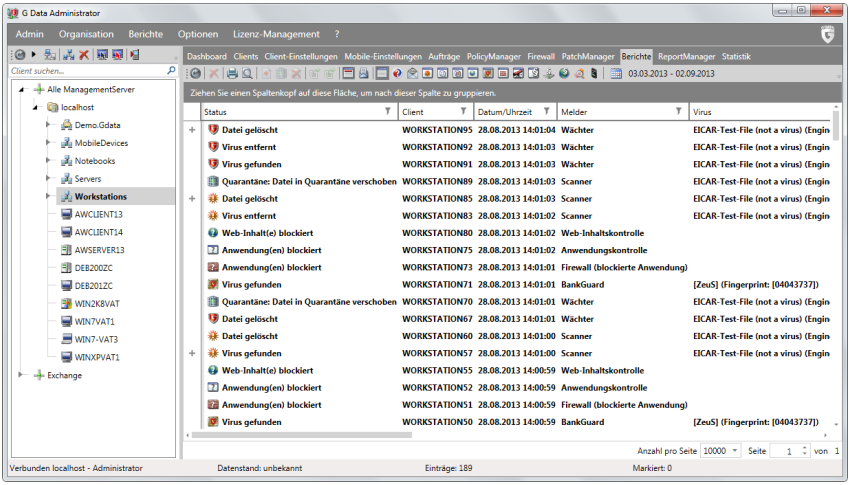
4.4.10. Berichte

Alle Meldungen der G Data-Software werden in diesem Aufgabenbereich angezeigt, wie zum Beispiel Virenfunde, Meldungen des PolicyManagers, PatchManager-Berichte sowie Firewall-Meldungen. Darüber hinaus werden zusätzlich systemrelevante Meldungen über Installationen, Berichte, Aufforderungen zum Neustart von Clients usw. hier aufgelistet. In der **Status**-Spalte der Liste wird der Berichtstyp angezeigt (z.B. **Virus gefunden** oder **Quarantine: Datei in Quarantäne verschoben**). Alle Berichte lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach unterschiedlichen Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.

Wenn Sie die Scanaufträge auf Ihrem System so eingestellt haben, dass diese den Virenbefall lediglich protokollieren, können Sie die Virenbekämpfung auch manuell

durchführen. Wählen Sie eine oder mehrere protokollierten Dateien und anschließend einen Befehl im Kontextmenü (rechte Maustaste), im Menü Berichte oder in der Symbolleiste. So lassen sich beispielsweise infizierte Dateien löschen oder in den Quarantäne-Ordner verschieben.

Über einige Berichte können Sie direkt einen Auftrag einplanen. Zum Beispiel: Falls ein Client einen Patch-Rollback angefordert hat, können Sie über **Details/Aktionen** das **Softwareverteilungs**-Fenster öffnen. Sie können dann direkt einen Rollback-Auftrag einplanen, ohne das PatchManager-Modul öffnen zu müssen.



Über das Berichte-Menü sind die folgenden Optionen verfügbar:

- **Ansicht**: Hier können Sie festlegen, ob Sie alle Berichte sehen möchten oder nur eine bestimmte Art von Berichten.
- **Abhängige Berichte ausblenden**: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.
- **Gelesene Berichte ausblenden**: Hier können Sie die Berichte ausblenden, die Sie schon gelesen haben.
- **Virus aus der Datei entfernen** (nur bei Virenfunden): Versucht den Virus aus der Originaldatei zu entfernen.
- **Datei in die Quarantäne verschieben** (nur bei Virenfunden): Diese Funktion verschiebt die ausgewählten Dateien in den Quarantäne-Ordner. Die Dateien werden verschlüsselt im Quarantäne-Ordner auf dem G Data ManagementServer gespeichert. Die Originaldateien werden gelöscht. Durch die Verschlüsselung ist sichergestellt, dass der Virus keinen Schaden anrichten kann. Beachten Sie, dass zu jeder Datei in der Quarantäne ein Bericht gehört.

Wenn Sie den Bericht löschen wird auch die Datei im Quarantäne-Ordner gelöscht. Sie können eine Datei aus dem Quarantäne-Ordner zur Untersuchung an den **Emergency-AntiViren Service** senden. Öffnen Sie dazu das Kontextmenü eines Quarantäne-Berichts mit einem Rechtsklick. In dem Berichtdialog klicken Sie dann nach Wahl des Einsendegrunds die Schaltfläche OK.

- **Datei löschen** (nur bei Virenfunden): Löscht die Originaldatei auf dem Client.
- **Quarantäne: Säubern und zurückbewegen** (nur bei Virenfunden): Es wird versucht, den Virus aus der Datei zu entfernen. Wenn dies gelingt, wird die gesäuberte Datei zurück an Ihren Ursprungsort auf dem jeweiligen Client bewegt. Wenn der Virus nicht entfernt werden kann, wird die Datei auch nicht zurückbewegt.
- **Quarantäne: Zurückbewegen** (nur bei Virenfunden): Verschiebt die Datei aus dem Quarantäne-Ordner zurück auf den Client. **Achtung**: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.
- **Quarantäne: An G Data Security Labs senden** (nur bei Virenfunden): Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.
- **Quarantäne: Datei und Bericht löschen** (nur bei Virenfunden): Löscht die gewählten Berichte und Quarantäne-Dateien.
- **Url auf die Whitelist setzen** (nur bei Berichten der **Web-Inhaltskontrolle**): Fügt den angeforderten URL zur Whitelist hinzu.
- **Url auf die Blacklist setzen** (nur bei Berichten der **Web-Inhaltskontrolle**): Fügt den angeforderten URL zur Blacklist hinzu.
- **Bericht löschen**: Hiermit löschen Sie die ausgewählten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine Quarantäne-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.
- **Abhängige Berichte löschen**: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die doppelten Einträge in der Protokolldatei löschen.

Die Symbolleiste des Berichte-Moduls bietet eine breite Palette von Optionen und Filter-Einstellungen:

Aktualisieren

Löschen

Drucken: Hiermit starten Sie den Druckvorgang für die Berichte. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche Sie ausdrucken lassen möchten.

Seitenansicht: Über die Seitenansicht-Funktion können Sie sich vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben lassen.

Virus entfernen

In Quarantäne verschieben

Datei löschen

Datei aus der Quarantäne zurückbewegen

Datei säubern und aus der Quarantäne zurückbewegen

Abhängige Berichte ausblenden

Gelesene Berichte ausblenden

Alle Berichte

Nur Fehler- und Informationsmeldungen

Nur Mail-Berichte

Nur Berichte mit nicht entfernten Viren

Nur Quarantäne-Berichte

Nur Inhalt der Quarantäne

Nur HTTP-Berichte

Nur BankGuard-Berichte

Nur Firewall-Berichte (falls Sie eine Softwareversion mit Firewall verwenden)

Nur Berichte der Verhaltensüberwachung

Nur Berichte der Anwendungskontrolle (falls Sie eine Softwareversion mit Anwendungskontrolle verwenden)

Nur Berichte der Gerätekontrolle (falls Sie eine Softwareversion mit Gerätekontrolle verwenden)

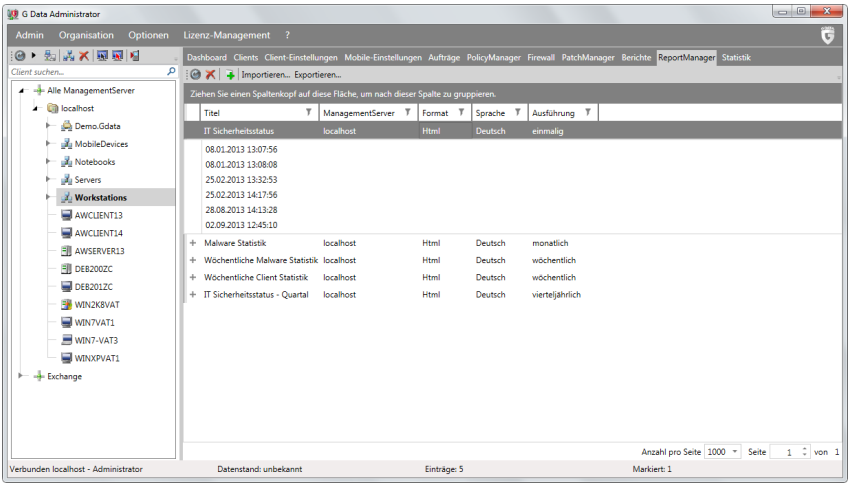
Nur Berichte der Web-Inhaltskontrolle (falls Sie eine Softwareversion mit Web-Inhaltskontrolle verwenden)

Nur PatchManagement-Berichte (falls Sie eine Softwareversion mit PatchManagement verwenden)

Nur MobileDeviceManagement-Berichte

4.4.11. ReportManager

Über den ReportManager können Sie zeitplangesteuert Berichte über den Status Ihrer Systemsicherheit konfigurieren und an ausgewählte Empfänger verteilen.



Aktualisieren

Löschen

Neue Reportplanung hinzufügen: Die Funktionen werden Ihnen im Kapitel **Reportdefinition** erläutert.

Über die Schaltfläche **Importieren** / **Exportieren** können Sie Einstellungen für den Report importieren und/oder exportieren. Führen Sie einen Rechtsklick auf einen oder mehrere Berichte durch um diese zu löschen oder - mit Auswahl von **Sofort ausführen** - auch direkt noch mal durchführen zu lassen. Um einen Bericht zu bearbeiten, klicken Sie auf **Eigenschaften**.

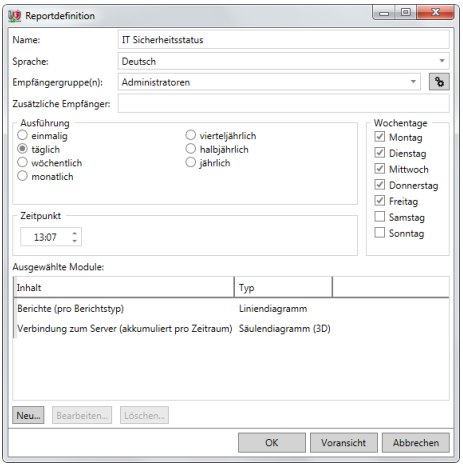
4.4.11.1. Reportdefinition

Hier kann festgelegt werden, welchen Namen der Report haben soll und in welcher Sprache er verfasst werden soll. Unter **Empfängergruppe(n)** können Sie festlegen, welche Liste von Empfängern diesen Report erhalten soll. Sie können dafür Gruppen verwenden, die Sie unter **Optionen** > **Server-Einstellungen** > **E-Mail** angelegt haben oder hier auch direkt neue Empfängergruppen definieren, darüber hinaus können Sie über das Eingabefeld **Zusätzliche Empfänger** auch weitere E-Mail-Adressen für den jeweiligen Report hinzufügen (Adressaten werden dabei durch Komma getrennt).

Bei einmaligen Reports können Sie eine Startzeit definieren, bei periodischen Reports

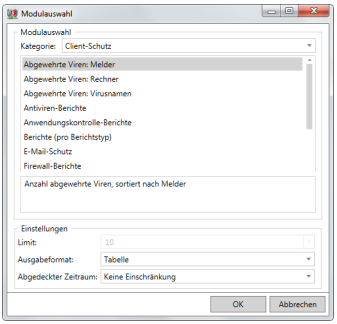
können Sie festlegen, in welchem Rhythmus die Benachrichtigung erfolgen soll.

> Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass ein Report nur an Werktagen durchgeführt wird oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.



Den Inhalt des jeweiligen Reports definieren Sie, indem Sie unter Ausgewählte Module auf die Schaltfläche **Neu** klicken und dort eins der auswählbaren Reportmodule aktivieren. Die Verfügbarkeit der Module ist abhängig von der Produktversion, die Sie verwenden. Die Module für die Reportplanung sind in drei Kategorien untergliedert: **Client-Allgemein**, **Client-Schutz** und **PatchManager**. Wählen Sie das entsprechende Modul und konfigurieren Sie die Einstellungen im unteren Bereich des Fensters. Für jedes Modul kann auch ein spezielles Ausgabeformat gewählt werden. Sie haben dabei die Auswahl aus **Tabelle**, **Liniendiagramm**, **Säulendiagramm (3D)** oder **Kuchendiagramm (3D)**. Bitte beachten Sie, dass nicht jedes Modul jedes Ausgabeformat unterstützt. Für manche Module können Sie außerdem ein **Limit** definieren, um die Menge der dargestellten Daten zu beschränken oder entsprechend einen zeitlichen Rahmen zur Darstellung auswählen. Klicken Sie auf **OK**, um die ausgewählten Module dem jeweiligen Bericht hinzuzufügen. Um Module zu bearbeiten oder zu löschen, stehen Ihnen die entsprechenden Schaltflächen zur Verfügung. Wenn Sie die Auswahl und Einstellung der Module abgeschlossen haben, können Sie sich unter **Voransicht** einen Beispielreport mit den getroffenen Einstellungen durchführen.

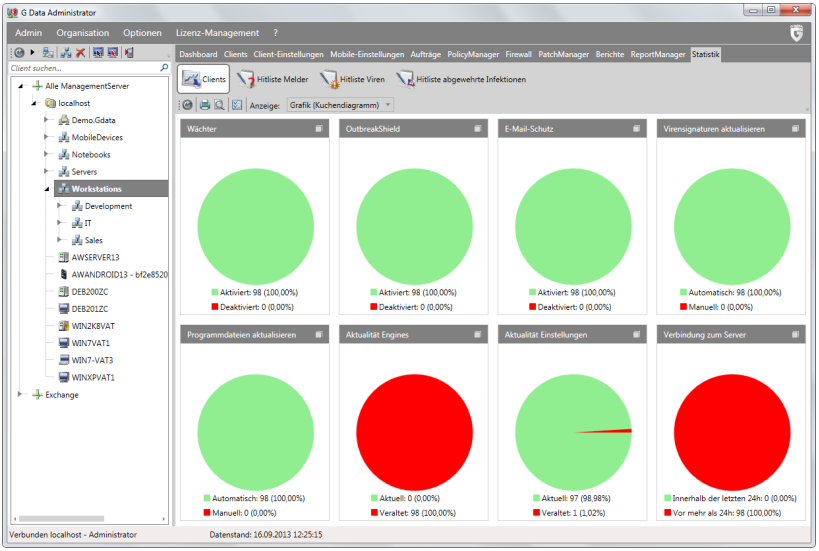
Wenn ein Report-Job durchgeführt wurde, erscheint der erstellte Report in der Übersicht des ReportManagers und wird an die ausgewählten Empfänger versendet. Um alle Instanzen eines Reports zu sehen, führen Sie einfach einen Doppelklick auf dem entsprechenden Report aus und öffnen Sie die zugehörigen Berichte.



Der Computer, auf dem G Data Administrator ausgeführt wird, muss über Internet Explorer 8 oder höher verfügen, um die Report-Voransicht und die Reportinstanzen-Ansicht anzeigen zu können.

4.4.12. Statistik

In diesem Aufgabenbereich können Sie sich statistische Informationen zum Virenaufkommen und zu Infektionen auf den Clients bzw. Exchange-Server anzeigen lassen, sowie den Sicherheitsstatus des verwalteten Netzwerks. Es stehen verschiedene Ansichten zur Verfügung: so kann die Darstellung der Informationen in Textform erfolgen oder auch grafisch aufbereitet werden (Säulen- oder Kuchendiagramm). Die entsprechende Ansicht lässt sich unter **Anzeige** auswählen. Es stehen Informationen bereit über die **Clients** (nicht verfügbar falls einen Exchange-Client selektiert wurde), über die **Hitliste Melder**, die **Hitliste Viren** und über die **Hitliste abgewehrte Infektionen**.



5. G Data WebAdministrator

Der G Data WebAdministrator ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden.

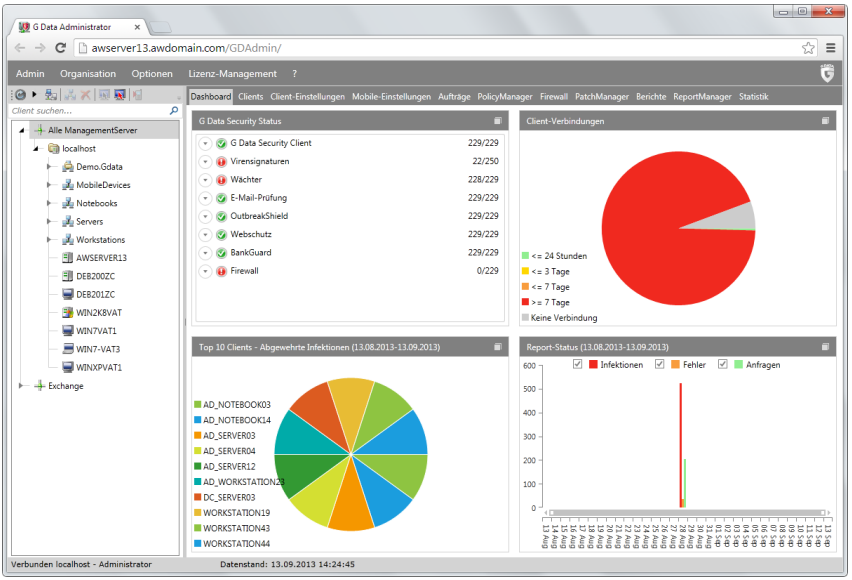
5.1. Starten des G Data WebAdministrators

Um den G Data WebAdministrator zu nutzen, klicken Sie auf das Desktop-Symbol des G Data WebAdministrators. Alternativ können Sie auch Ihren Internetbrowser starten und die URL ansurfen, die Ihnen beim Abschluss des Installationsprozesses mitgeteilt wurde. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem IIS ausgeführt wird und der WebAdministrator installiert wurde, sowie dem Ordner-Suffix (z.B. *http://10.0.2.150/GDAdmin/*). Wenn Sie bis jetzt das Microsoft Silverlight Browser Plugin noch nicht installiert haben, werden Sie nun dazu aufgefordert, es herunterzuladen.

Nun öffnet sich automatisch eine Anmeldeseite für den Zugang zum G Data WebAdministrator. Geben Sie hier nun wie beim regulären G Data Administrator Ihre Zugangsdaten ein und klicken Sie dann auf die Schaltfläche **OK**.

5.2. Verwendung des G Data WebAdministrators

Die Programmoberfläche des G Data WebAdministrators ist sehr ähnlich zur Oberfläche des G Data Administrators. Nach dem Einloggen sehen Sie das zentrale Dashboard, welches Ihnen einen Überblick über Ihr Netzwerk, die Clients und den Zustand des G Data ManagementServers bietet.



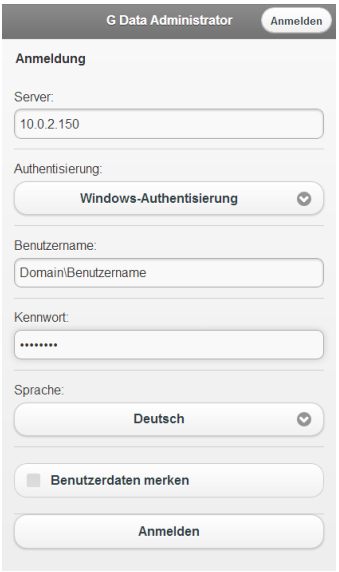
Die Funktionen des WebAdministrators sind identisch zu denen des G Data Administrators. Diese werden im Kapitel **G Data Administrator** umfangreich beschrieben.

6. G Data MobileAdministrator

Der G Data MobileAdministrator ist die über Smartphones bedienbare Programmoberfläche des G Data ManagementServers. Es kann zum schnellen Bearbeiten und Updaten von Einstelllungen verwendet werden und ist für die Nutzung mit mobilen Geräten optimiert. Dazu sind die wichtigsten und am häufigsten benutzten Funktionen des G Data Administrators so zusammengestellt worden, dass Sie auf einer breiten Palette unterschiedlichster Smartphone-Umgebungen genutzt werden können.

6.1. Starten des G Data MobileAdministrators

Nach Abschluss der Installation des G Data MobileAdministrators können Sie diesen von jedem Browser aus aufrufen. Starten Sie dazu Ihren Browser und wählen die URL aus, die Ihnen am Ende des Installationsprozesses mitgeteilt wird. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem IIS ausgeführt wird und der WebAdministrator installiert wurde, sowie dem Ordner-Suffix (z.B. *http://10.0.2.150/GDMobileAdmin/*).



Die Anmeldeseite des MobileAdministrators ist genauso aufgebaut wie die Anmeldeseite des **G Data Administrators** und des **G Data WebAdministrators**. Geben Sie hier bitte den **Server**, den **Benutzernamen**, Ihr **Kennwort** und Ihre **Benutzersprache** an. Wählen Sie die **Windows-Authentisierung**, wenn Sie sich mit Ihren Windows-(Domain-)Zugangsdaten anmelden möchten oder die **Integrierte Authentisierung**, wenn Sie Ihre Zugangsdaten direkt über den Administrator verwalten lassen. Sollten Sie wünschen, dass Ihre Zugangsdaten (bis auf das Kennwort) beim nächsten Öffnen der Anmeldeseite wieder zur Verfügung stehen, wählen Sie

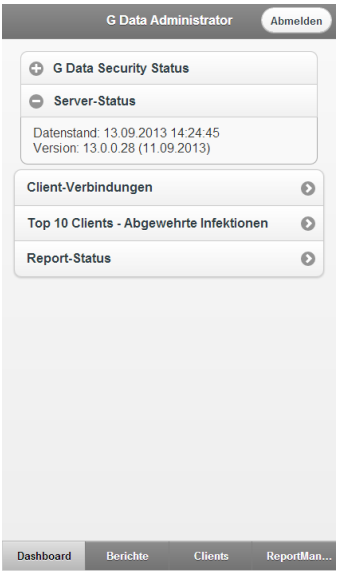
bitte **Benutzerdaten merken**.

6.2. Verwendung des G Data MobileAdministrators

Nach dem Einloggen am G Data MobileAdministrator wird das Hauptmenü angezeigt. Hier stehen Ihnen vier Optionen zur Verfügung: **Dashboard**, **Berichte**, **Clients**, und **ReportManager**. Um das Programm zu beenden, tippen Sie auf die Schaltfläche **Abmelden** oben rechts.

6.2.1. Dashboard

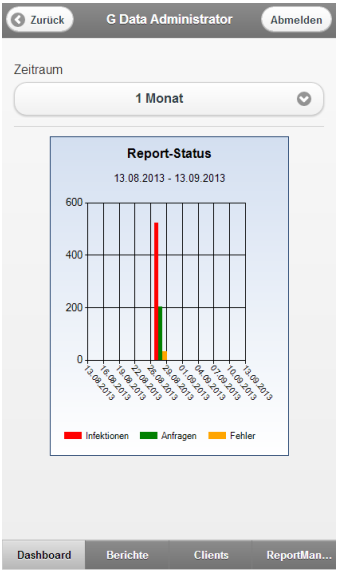
Im Dashboard des G Data MobileAdministrators können Sie die wichtigsten Statistiken über Ihr Netzwerk auf einem Blick einsehen. Vergleichbar mit der Dashboard-Ansicht im G Data Administrator haben Sie hier einen Überblick über den G Data ManagementServer und dessen Clients. Zusätzlich können Sie sich hier Statistiken über Client-Verbindungen und verhinderte Infektionen anzeigen lassen.



Wählen Sie die Ansicht **G Data Security Status** um eine genauere Übersicht über den Status von Server und Clients zu erhalten. Der MobileAdministrator zeigt Ihnen, wie viele Clients mit dem G Data Security Client ausgestattet sind und bietet Ihnen Informationen über den Aktualisierungsstatus der Virensignaturen und anderer Programmkomponenten (z.B. OutbreakShield, Firewall und Wächter). Sie können über das Öffnen des Virus-Signatur-Unterbereichs auch direkt Engine-Rollbacks durchführen. Der Zustand des ManagementServers an sich kann unter **Server-Status** genauer betrachtet werden.

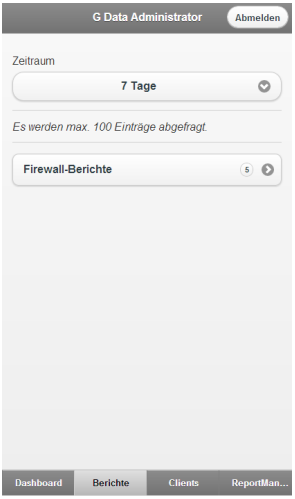
Weitere Statistiken erhalten Sie unter **Client-Verbindungen** und **Top 10 Clients -**

Abgewehrte Infektionen. Tippen Sie auf **Report-Status**, um sich Informationen über Infektionen, Anfragen und Error reports anzeigen zu lassen.



6.2.2. Berichte

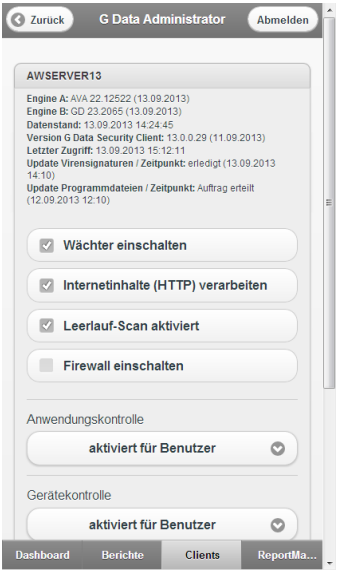
In der Berichte-Ansicht finden Sie Reports über Viren, Firewall-Ereignisse und Meldungen des PolicyManagers. Hierbei handelt es sich um eine für mobile Geräte optimierte Darstellung derselben Informationen, die Sie auch im G Data Administrator im **Berichte**-Bereich finden.



Wählen Sie unter **Zeitraum** aus, ob Sie die Reports des letzten Tages, der letzten sieben Tage oder des letzten Monats angezeigt bekommen möchten. Der MobileAdministrator zeigt Ihnen dann an, für welche Kategorie Berichte vorliegen. Wenn Sie eine dieser Kategorien antippen, erhalten Sie eine Übersicht über die aufgezeichneten Ereignisse. Berichte können nach Namen gefiltert werden.

6.2.3. Clients

Der MobileAdministrator bietet Ihnen einen genauen Überblick über alle Clients, die vom G Data ManagementServer verwaltet werden. Für jeden Client sind Detailinformationen abrufbar und wichtige Sicherheitseinstellungen können direkt über den MobileAdministrator verändert werden.

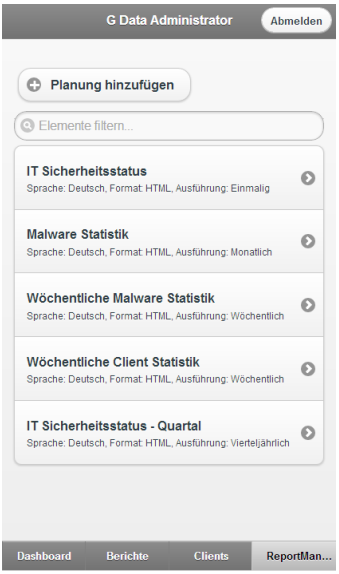


In der Übersichtsanzeige können Sie sich eine Liste aller Rechner anzeigen lassen, welche durch den G Data ManagementServer verwaltet werden. Diese Liste kann auch nach Namen gefiltert werden. Wenn Sie einen Client gezielt auswählen, können Sie gezielt für diesen Statistiken über Versionen und Updates einsehen. Darüber hinaus können wichtige Sicherheitseinstellungen direkt verändert werden. So können Sie den **Wächter** ein- oder ausschalten, bestimmen ob **Internetinhalte (HTTP)** verarbeitet werden sollen oder nicht, den **Leerlauf-Scan** aktivieren oder deaktivieren und die **Firewall** ein- oder ausschalten.

Über den Bereich Clients können darüber hinaus **Anwendungskontrolle**, **Gerätekontrolle**, **Web-Inhaltskontrolle**, und **Internetnutzungszeit** kontrolliert und editiert werden.

6.2.4. ReportManager

Beim ReportManager handelt es sich um die mobile Version des **ReportManager**-Bereichs im G Data Administrator. Hier haben Sie die Möglichkeit, Berichte zu konfigurieren, zu timen und in einer Vorschau zu betrachten.



Um eine neuen Report-Auftrag hinzuzufügen, tippen Sie auf **Planung hinzufügen**. Schon vorhandene Reports können Sie durch einfaches Antippen zum Editieren auswählen. Dabei stehen Ihnen alle Einstellungsmöglichkeiten zur Verfügung, die auch im ReportManager der Desktopversion möglich sind.

7. G Data Security Client

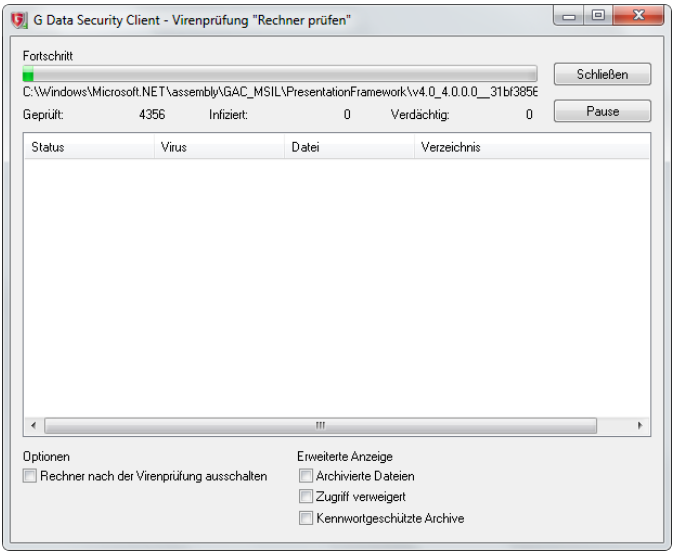
Die Client-Software stellt den Schutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Clients verfügen über eigene Virensignaturen und einen eigenen Scheduler, damit auch im Offline-Betrieb (z.B. bei Notebooks, die keine ständige Verbindung zum G Data ManagementServer haben) Virenanalysen durchgeführt werden können.

Nach der Installation der Client-Software steht dem Benutzer des Clients ein Symbol in der Startleiste zur Verfügung, über welches er unabhängig von den Zeitplänen des Administrators auch selber auf Virenschutz-Funktionen zugreifen kann. Welche Funktionen dem Nutzer zur Verfügung stehen, definieren Sie als Administrator im Bereich **Client-Einstellungen** des G Data Administrators.

Über die rechte Maustaste kann der Benutzer auf diesem G Data Security Client-Symbol ein Kontextmenü öffnen, das Zugriff auf alle Funktionen anbietet.

7.1. Virenprüfung

Über diese Option kann der Anwender gezielt mit dem G Data Security Client seinen Rechner auch außerhalb der im G Data Administrator vorgegebenen Prüfzeiträume auf Viren überprüfen.



Der Anwender kann zusätzlich Disketten, CDs/DVDs, den Speicher und Autostart-Bereich, sowie einzelne Dateien oder Verzeichnisse prüfen. Auf diese Weise können

auch Notebook-Nutzer, die ihren Rechner nur selten mit dem Firmennetzwerk verbinden, gezielt einen Virenbefall des Systems unterbinden. Über das **Optionen**-Fenster können Client-User so festlegen, welche Aktionen bei einem Virenfund durchgeführt werden sollen (z.B. Verschieben der Datei in den Quarantäne-Bereich.

> Der Anwender kann auch aus dem Windows-Explorer heraus Dateien oder Verzeichnisse überprüfen, indem er diese markiert und dann in dem Kontextmenü der rechten Maustaste die Funktion **Auf Viren prüfen (G Data AntiVirus)** verwendet.

Während einer laufenden Virenprüfung wird das Kontextmenü um folgende Einträge erweitert:

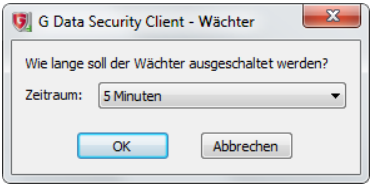
- **Priorität Virenprüfung**: Der Anwender hat hier die Möglichkeit, die Priorität der Virenprüfung festzulegen. Bei **Hoch** erfolgt die Virenprüfung schnell, allerdings kann sich das Arbeiten mit anderen Programmen an diesem Rechner deutlich verlangsamen. Bei der Einstellung **Niedrig** dauert die Virenprüfung hingegen vergleichsweise lange, dafür kann währenddessen, ohne größere Einschränkungen, am Client-Rechner weitergearbeitet werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.
- **Virenprüfung anhalten**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eingenständig anzuhalten. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann angehalten werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Virenprüfung abbrechen**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eingenständig abzubrechen. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann abgebrochen werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Scanfenster anzeigen**: Hiermit kann sich der Anwender das Info-Fenster anzeigen lassen, in dem Verlauf und Fortschritt der Virenprüfung angezeigt werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.

Die Option Virenprüfung kann im G Data Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.2. Wächter ausschalten

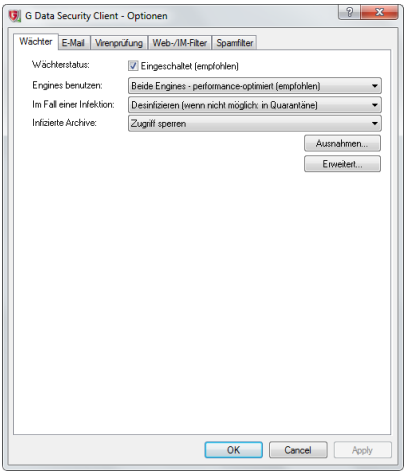
Über diesen Befehl kann der G Data Wächter vom Anwender für einen gewissen Zeitraum (von 5 Minuten bis zum nächsten Neustart des Rechners) ausgeschaltet werden. Das zeitweilige Ausschalten kann bei umfangreichen Dateikopiervorgängen sinnvoll sein, da auf diese Weise der Kopiervorgang beschleunigt wird. Der Echtzeit-Virenschutz ist in diesem Zeitraum allerdings ausgeschaltet.

Die Option Wächter ausschalten kann im G Data Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.



7.3. Optionen

Der Benutzer des Client-Rechners hat unter Optionen die Möglichkeit, selber Einstellungen in folgenden Bereichen für seinen Client zu ändern: **Wächter**, **Email**, **Virenprüfung** (lokal), **Web/IM** und **AntiSpam**. Auf diese Weise können sämtliche Schutzmechanismen der G Data Software auf dem Client ausgeschaltet werden. Diese Option sollte nur fachlich versierten Anwendern zugänglich sein. Die einzelnen Einstellungsmöglichkeiten werden ausführlich im Bereich **Client-Einstellungen** erläutert.



Die verschiedenen Karteikarten können im G Data Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.4. Quarantäne

Jeder Client hat einen lokalen Quarantäneordner, in den infizierte Dateien (abhängig von den Einstellungen für Wächter/Scanauftrag) verschoben werden können. Eine Datei, die in Quarantäne verschoben wurde, kann, sofern sie einen Virus enthält, keine Schadroutinen ausführen. Infizierte Dateien werden beim Verschieben in die Quarantäne automatisch gepackt und verschlüsselt. Für die Quarantäne bestimmte

Dateien, die größer sind als 1 MB werden automatisch immer in der lokalen Quarantäne des Clients abgelegt, um bei einem massiven Virenbefall das Netzwerk nicht unnötig zu belasten. Alle Dateien, die kleiner als 1 MB sind, werden an den Quarantäneordner des G Data ManagementServers übertragen. Diese Einstellungen sind nicht veränderbar. Die Client-Quarantäne befindet sich im Verzeichnis %ProgramData% \G DATA\AntiVirusKit Client\Quarantine. Die G Data ManagementServer-Quarantäne befindet sich im Verzeichnis %ProgramData%\G DATA\AntiVirus ManagementServer \Quarantine.

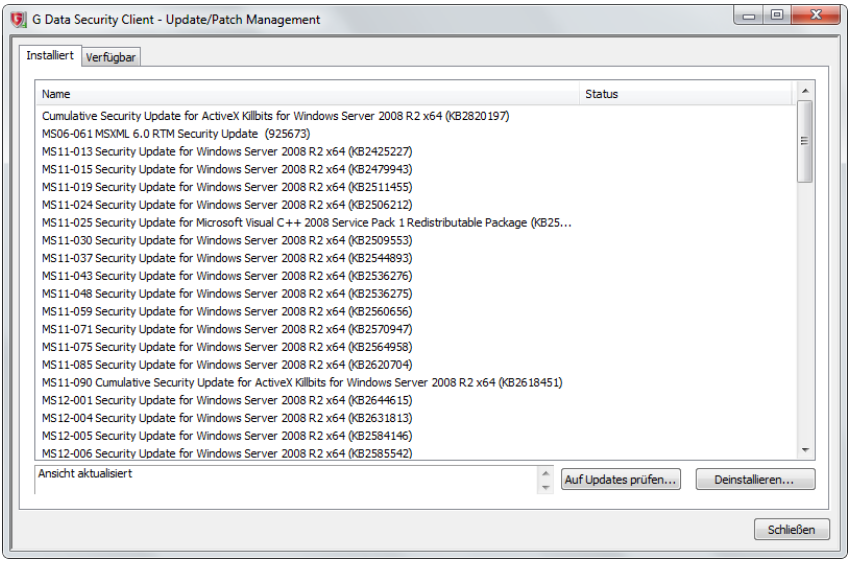
Sollten auf einem mobilen Client ohne Verbindung zum G Data ManagementServer eine infizierte Datei gefunden werden, die kleiner ist als 1 MB, wird sie in der lokalen Quarantäne gespeichert und erst beim nächsten Kontakt zum G Data ManagementServer in die dortige Quarantäne übertragen. Im Quarantäne-Ordner können befallene Dateien desinfiziert werden. Wenn dies nicht funktioniert, lassen sich die Dateien von dort auch löschen und ggf. aus der Quarantäne an ihren Ursprungsort zurückbewegen.

> **Achtung**: Beim Zurückbewegen wird ein Virus nicht entfernt. Sie sollten diese Option nur wählen, wenn das Programm ohne die befallene Datei nicht lauffähig ist und Sie diese trotzdem zur Datenrettung benötigen.

Die Option Quarantäne kann im G Data Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.

7.5. Updates/Patches

Hinter der Option Updates/Patches findet sich eine Übersicht der Updates und Patches für den Client-PC.


G Data Security Client - Update/Patch Management
Installiert
Verfügbar
Name
Status
Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 (KB2820197)
MS06-061 MSXML 6.0 RTM Security Update (925673)
MS11-013 Security Update for Windows Server 2008 R2 x64 (KB2425227)
MS11-015 Security Update for Windows Server 2008 R2 x64 (KB2479943)
MS11-019 Security Update for Windows Server 2008 R2 x64 (KB2511455)
MS11-024 Security Update for Windows Server 2008 R2 x64 (KB2506212)
MS11-025 Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB25...
MS11-030 Security Update for Windows Server 2008 R2 x64 (KB2509553)
MS11-037 Security Update for Windows Server 2008 R2 x64 (KB2544893)
MS11-043 Security Update for Windows Server 2008 R2 x64 (KB2536276)
MS11-048 Security Update for Windows Server 2008 R2 x64 (KB2536275)
MS11-059 Security Update for Windows Server 2008 R2 x64 (KB2560656)
MS11-071 Security Update for Windows Server 2008 R2 x64 (KB2570947)
MS11-075 Security Update for Windows Server 2008 R2 x64 (KB2564958)
MS11-085 Security Update for Windows Server 2008 R2 x64 (KB2620704)
MS11-090 Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 (KB2618451)
MS12-001 Security Update for Windows Server 2008 R2 x64 (KB2644615)
MS12-004 Security Update for Windows Server 2008 R2 x64 (KB2631813)
MS12-005 Security Update for Windows Server 2008 R2 x64 (KB2584146)
MS12-006 Security Update for Windows Server 2008 R2 x64 (KB2585542)
Ansicht aktualisiert
Auf Updates prüfen...
Deinstallieren...
Schließen

Auf der Registerkarte **Installiert** sehen Sie alle Patches und Updates, welche auf dem System installiert worden sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie ausführliche Informationen zum jeweiligen Patch oder Update. Sollte ein Patch oder Update Probleme machen, kann der Anwender es über die Schaltfläche **Deinstallieren** markieren und automatisch dem Administrator zur Deinstallation vorschlagen. Der **Status** des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Rollback-Anfrage. Unabhängig von eventuellen zeit- oder ferngesteuerten Softwareerkennungs-Jobs kann der Anwender über die Schaltfläche **Auf Updates prüfen** auch selber nach aktuellen Patches für sein System suchen.

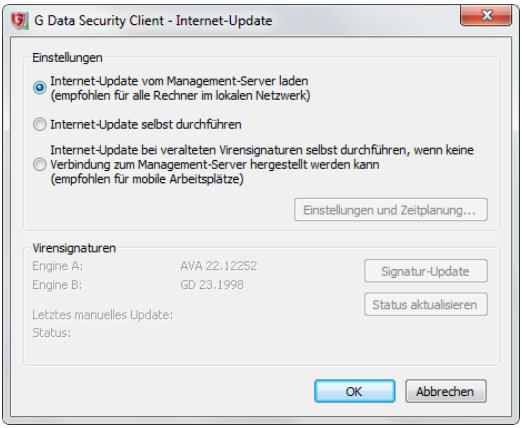
Auf der Registerkarte **Verfügbar** werden alle Software-Pakete, Patches und Upgrades angezeigt, die für den Client verfügbar sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie ausführliche Informationen zum jeweiligen Patch oder Update. Um als Client-Nutzer die Installation aktualisierter Programmdaten zu initiieren, kann dieser hier auf **Installieren** klicken. Der **Status** des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Distributionsanfrage.

Die Option Updates/Patches kann im G Data Administrator unter **PatchManager** > **Einstellungen** ein- und ausgeschaltet werden.

7.6. Internet-Update

Über den G Data Security Client können auch vom Client-Rechner aus selbstständig Internet-Updates der Virensignaturen durchgeführt werden, falls keine Verbindung zum G Data ManagementServer besteht. Über die Schaltfläche **Einstellungen und Zeitplanung** kann auch die Aktualisierung der Virensignaturen auf dem Client zeitgesteuert ablaufen.

Die Option Internet-Update kann im G Data Administrator unter **Client-Einstellungen** > **Allgemein** > **Client-Funktionen** ein- und ausgeschaltet werden.



7.7. Firewall ausschalten

Über **Firewall ausschalten** kann die Firewall ausgeschaltet werden, auch wenn der Client sich noch im ManagementServer-Netzwerk befindet. Wenn die Firewall ausgeschaltet ist, kann sie über die Option **Firewall einschalten** wieder eingeschaltet werden.

Die Option Firewall ausschalten kann im G Data Administrator unter **Firewall** > **Übersicht** ein- und ausgeschaltet werden (**Der Benutzer darf die Firewall ein- und ausschalten**).

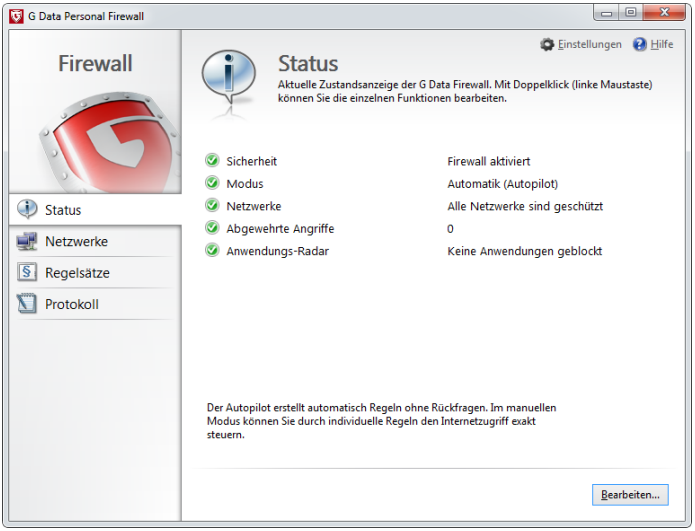
7.8. Firewall

Der Menüeintrag Firewall öffnet das Interface der Firewall. Solange sich der Client im Netzwerk des G Data ManagementServers befindet, wird die Firewall zentral vom Server aus administriert. Sobald der Client sich mit einem anderen Netzwerk verbindet, z.B. wenn ein Firmenlaptop zu Hause verwendet wird, kann das Firewall-Interface genutzt werden, um die Offsite-Konfiguration zu ändern.

Der Menüeintrag Firewall kann im G Data Administrator unter **Firewall** > **Übersicht** ein- und ausgeschaltet werden (**Der Benutzer darf die Offsite-Konfiguration ändern**).

7.8.1. Status

Im Status-Bereich erhalten Sie grundlegende Informationen zum aktuellen Zustand der Firewall. Durch doppeltes Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln.

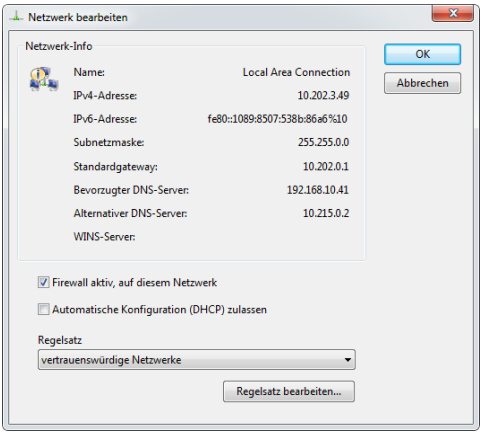


- **Sicherheit**: Firewall aktivieren oder deaktivieren. Diese Funktion ist nur verfügbar falls der Administrator diese im G Data Administrator erlaubt hat (**Firewall** > **Übersicht** > **Der Benutzer darf die Firewall ein- und ausschalten**).
- **Modus**: Die Firewall kann mit automatischer (Autopilot) oder manueller Regelerstellung betrieben werden. Diese Funktion kann clientseitig nur geändert werden falls der Client außerhalb des ManagementServer-Netzwerks verwendet wird und der Administrator das Einstellen dieser Funktion im G Data Administrator erlaubt hat (**Firewall** > **Übersicht** > **Der Benutzer darf die Offsite-Konfiguration ändern**).
- **Netzwerke**: Öffnet den **Netzwerke**-Bereich. Hier können Sie sich die Netzwerke, in denen sich Ihr Computer befindet, sowie die verwendeten Regelsätze anzeigen lassen.
- **Abgewehrte Angriffe**: Sobald die Firewall einen Angriff auf Ihren Computer registriert, wird dieser verhindert und hier protokolliert.
- **Anwendungs-Radar**: Dieses Dialogfeld zeigt Ihnen, welche Programme momentan von der Firewall blockiert werden. Sollten Sie einer der blockierten Anwendungen doch die Erlaubnis für die Nutzung des betreffenden Netzwerkes erteilen wollen, wählen Sie diese hier einfach aus und klicken Sie dann die Schaltfläche **Erlauben** an.

7.8.2. Netzwerke

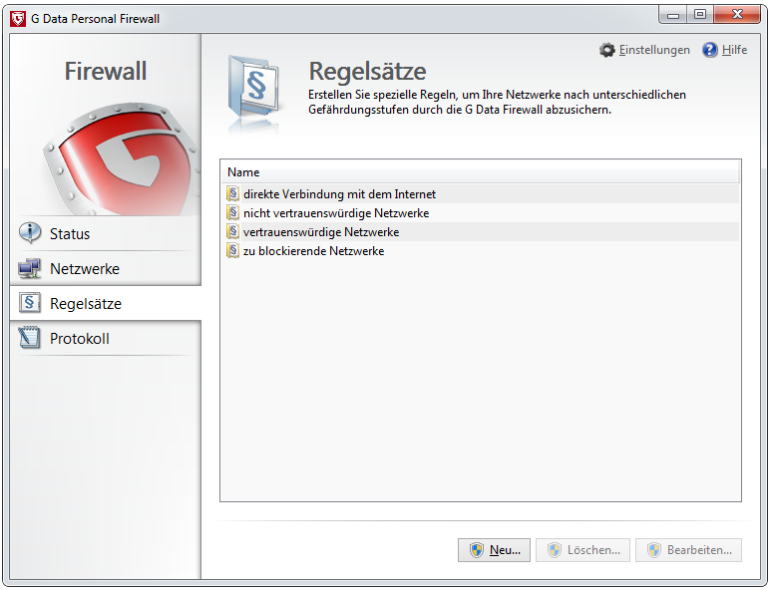
Im Netzwerke-Bereich werden alle Netzwerke (z.B. LAN, DFÜ etc.) aufgelistet, mit denen der Rechner verbunden ist. Hier wird auch aufgezeigt, mit welchem Regelsatz das jeweilige Netzwerk geschützt wird. Wenn Sie ein Netzwerk mit der Maus markieren und die **Bearbeiten**-Schaltfläche anklicken, können Sie die Firewall-Einstellungen für dieses Netzwerk einsehen, bzw. verändern. Einstellungen können nur geändert werden, falls der Administrator dies erlaubt hat (**Firewall** > **Übersicht** > **Der Benutzer darf die Firewall ein- und ausschalten**) oder der Client im Offsite-Modus verwendet wird (**Firewall** > **Übersicht** > **Der Benutzer darf die Offsite-Konfiguration ändern**).

- **Netzwerk-Info**: Zeigt Netzwerk-Informationen wie IP-Adresse, Subnetzmaske, Standardgateway, DNS- und WINS-Server.
- **Firewall aktiv, auf diesem Netzwerk**: Firewall aktivieren oder deaktivieren.
- **Gemeinsame Nutzung der Internet Verbindung**: Internetverbindungsfreigabe (ICS) erlauben oder sperren.
- **Automatische Konfiguration (DHCP) zulassen**: Automatische IP-Konfiguration (DHCP) erlauben oder sperren.
- **Regelsatz**: Wählen Sie den **Regelsatz**, der für dieses Netzwerk verwendet werden sollte. Wählen Sie **Regelsatz bearbeiten**, um den **Regelassistenten** zu öffnen.



7.8.3. Regelsätze

In diesem Bereich können Sie Regelsätze anlegen und bearbeiten. Regelsätze enthalten Firewall-Regeln und können einem oder mehreren Netzwerken zugewiesen werden.



- **Neu**: Neuen Regelsatz hinzufügen. Legen Sie in dem erscheinenden Dialogfenster den **Regelsatz Name** fest und entscheiden Sie sich, ob grundlegende Regeln für nicht vertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen.
- **Löschen**: Regelsatz löschen. Die vorgegebenen Regelsätze für direkte

Verbindung mit dem Internet, vertrauenswürdige Netzwerke, nicht vertrauenswürdige Netzwerke und zu blockierende Netzwerke können nicht gelöscht werden.

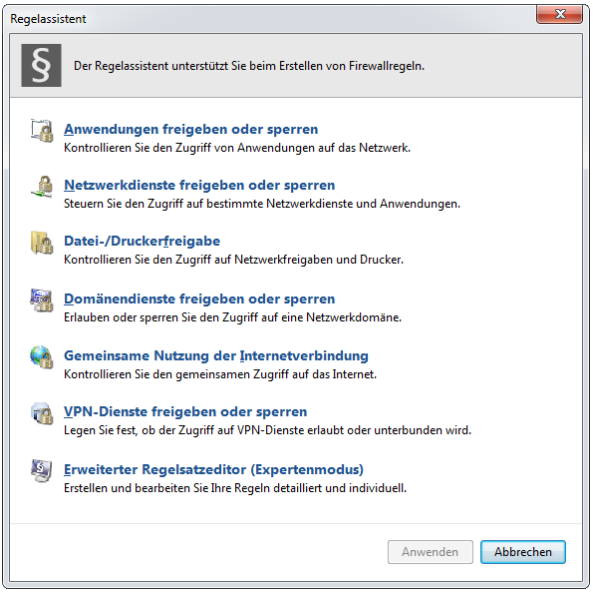
- **Bearbeiten**: Regelsatz bearbeiten mit dem **Regelassistenten**.

Der Bereich Regelsätze beinhaltet voreingestellte Regelsätze für folgende Netzwerktypen:

- **Direkte Verbindung mit dem Internet**: Hierunter fallen Regeln, die den direkten Internetzugriff behandeln.
- **Nicht vertrauenswürdige Netzwerke**: Hierunter fallen vor allem offene Netzwerke, wie z.B. DFÜ-Netzwerke, die auf das Internet Zugriff haben.
- **Vertrauenswürdige Netzwerke**: Vertrauenswürdig sind in der Regel Heim- und Firmennetzwerke.
- **Zu blockierende Netzwerke**: Wenn zeitweise oder dauerhaft der Kontakt des Rechners zu einem Netzwerk blockiert werden soll, kann dieser Regelsatz verwendet werden.

7.8.3.1. Regelassistent

Mit dem Regelassistenten können Sie Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln ändern. Der Regelassistent ist besonders geeignet für Anwender, die sich nicht gut mit der Firewall-Technologie auskennen. Fur eine genauere Kontrolle über individuelle Regeln verwenden Sie den **Erweiterten Regelsatzeditor**.


Regelassistent
Der Regelassistent unterstützt Sie beim Erstellen von Firewallregeln.
Anwendungen freigeben oder sperren
Kontrollieren Sie den Zugriff von Anwendungen auf das Netzwerk.
Netzwerkdienste freigeben oder sperren
Steuern Sie den Zugriff auf bestimmte Netzwerkdienste und Anwendungen.
Datei-/Druckerfreigabe
Kontrollieren Sie den Zugriff auf Netzwerkfreigaben und Drucker.
Domänendienste freigeben oder sperren
Erlauben oder sperren Sie den Zugriff auf eine Netzwerkdomäne.
Gemeinsame Nutzung der Internetverbindung
Kontrollieren Sie den gemeinsamen Zugriff auf das Internet.
VPN-Dienste freigeben oder sperren
Legen Sie fest, ob der Zugriff auf VPN-Dienste erlaubt oder unterbunden wird.
Erweiterter Regelsatzeditor (Expertenmodus)
Erstellen und bearbeiten Sie Ihre Regeln detailliert und individuell.
Anwenden
Abbrechen

Der Regelassistent bietet verschiedene Regeln, mit denen Sie schnell und unkompliziert einen bestimmten Verbindungstyp erlauben oder sperren können. Für die meisten Regeln können Sie eine **Richtung** definieren, die bestimmt ob eine Regel eingehende und/oder ausgehende Verbindungen blockiert.

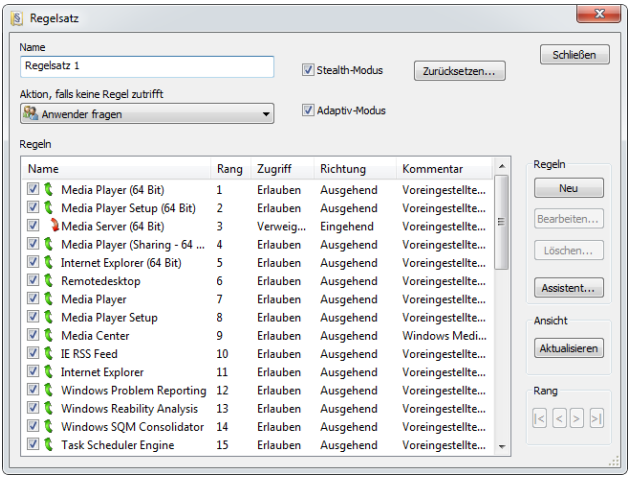
- **Anwendungen freigeben oder sperren**: Erlauben oder Sperren des Zugriffs einer Anwendung auf das Netzwerk, für das den Regelsatz definiert wurde.
- **Netzwerkdienste freigeben oder sperren**: Über das Sperren eines oder mehrerer Ports können schnell Lücken geschlossen werden, die sonst von Hackern für Angriffe genutzt werden könnten. Im Assistenten haben Sie die Möglichkeit Ports komplett oder nur für eine bestimme Anwendung zu sperren.
- **Datei-/Druckerfreigabe**: Ordner- und Druckerfreigabe erlauben oder sperren.
- **Domänendienste freigeben oder sperren**: Netzwerkdomänendienste erlauben oder sperren.
- **Gemeinsame Nutzung der Internetverbindung**: Internetverbindungsfreigabe (ICS) erlauben oder sperren.
- **VPN-Dienste freigeben oder sperren**: Virtual Private Network (VPN)-Dienste erlauben oder sperren.
- **Erweiterter Regelsatzeditor (Expertenmodus)**: Öffnet den **Erweiterten Regelsatzeditor**.

7.8.3.2. Erweiterter Regelsatzeditor

Mit dem erweiterten Regelsatzeditor können Sie sehr individuelle Regeln für das jeweilige Netzwerk definieren. Dabei können sämtliche Regeln erzeugt werden, die Sie auch über den Regelassistenten erzeugen können, aber auch darüber hinaus weitergehende Einstellungen vorgenommen werden.

Der erweiterte Regelsatzeditor ähnelt dem **Regelsätze**-Bereich des G Data Administrator **Firewall**-Moduls. Sie können den Editor verwenden, um Regeln zu erstellen, zu bearbeiten und zu löschen, sowie um Regeln nach Rang einzuteilen. Neben den auch im G Data Administrator verfügbaren Möglichkeiten bietet der erweiterte Regelsatzeditor die folgenden Funktionen:

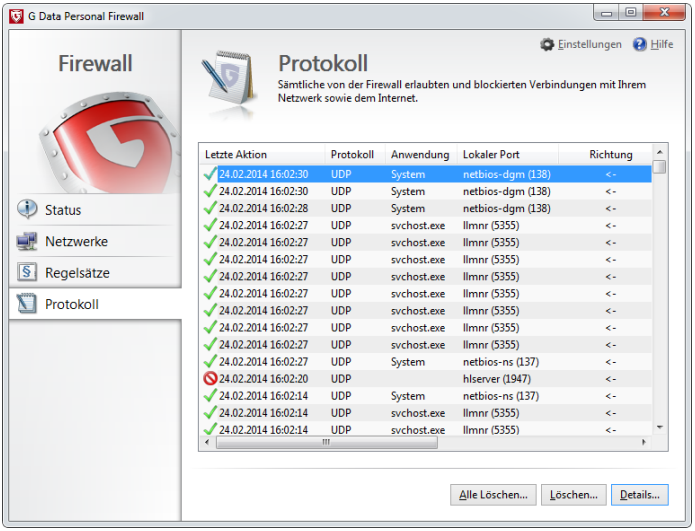
- **Aktion, falls keine Regel zutrifft**: Hier können Sie festlegen, ob der Zugriff im Netzwerk generell erlaubt, verweigert oder auf Nachfrage geregelt werden soll.
- **Adaptiv-Modus**: Der Adaptiv-Modus unterstützt Sie bei Anwendungen, die die sogenannte Rückkanal-Technik verwenden (z.B. FTP und viele Online-Spiele). Solche Anwendungen verbinden sich mit einem entfernten Rechner und handeln mit ihm einen Rückkanal aus, auf dem sich der entfernte Rechner mit Ihrer Anwendung zurückverbindet. Ist der Adaptiv-Modus aktiv, so erkennt die Firewall diesen Rückkanal und lässt ihn zu, ohne gesondert nachzufragen.
- **Zurücksetzen**: Löscht alle Änderungen sowie erlernte Regeln.



Einzelne Regeln können bearbeitet werden, indem Sie die Regel wählen und die **Bearbeiten**-Taste drücken. Das Regelbearbeitungsfenster ist identisch mit dem Fenster **Regel bearbeiten** im G Data Administrator.

7.8.4. Protokoll

Der Bereich Protokoll zeigt eine detaillierte Übersicht mit allen eingehenden und ausgehenden Verbindungen. Sie können den Bereich verwenden zur: Überprüfung von Verbindungsprotokoll, Anwendung, Richtung, lokalem Port, entferntem Host, entferntem Port und dem Grund für die Entscheidung, die Verbindung zu blockieren oder zu erlauben.

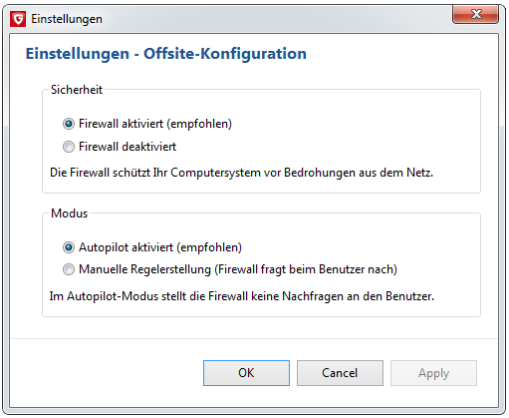

G Data Personal Firewall
Einstellungen
Hilfe
Firewall
Status
Netzwerke
Regelsätze
Protokoll
Protokoll
Sämtliche von der Firewall erlaubten und blockierten Verbindungen mit Ihrem Netzwerk sowie dem Internet.
Letzte Aktion Protokoll Anwendung Lokaler Port Richtung
24.02.2014 16:02:30 UDP System netbios-dgm (138) <-
24.02.2014 16:02:30 UDP System netbios-dgm (138) <-
24.02.2014 16:02:28 UDP System netbios-dgm (138) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:27 UDP System netbios-ns (137) <-
24.02.2014 16:02:20 UDP hlserver (1947) <-
24.02.2014 16:02:14 UDP System netbios-ns (137) <-
24.02.2014 16:02:14 UDP svchost.exe llmnr (5355) <-
24.02.2014 16:02:14 UDP svchost.exe llmnr (5355) <-
Alle Löschen...
Löschen...
Details...

Wählen Sie **Löschen**, um einen einzelnen Protokolleintrag zu löschen oder **Alle Löschen**, um alle Einträge zu löschen. Die Schaltfläche **Details** zeigt Ihnen weitere Informationen über den ausgewählten Eintrag.

Klicken Sie mit der rechten Maustaste auf einen Eintrag, um Zugriff auf weitere Optionen zu erhalten. Neben dem **Details**-Fenster, können Sie auch neue Regeln erstellen, bestehende Regeln bearbeiten und einen Filter für die Protokollansicht definieren.

7.8.5. Einstellungen

Das Fenster Einstellungen kann nur dann benutzt werden, wenn der Administrator die entsprechenden Berechtigungen eingestellt hat (**Firewall** > **Übersicht** > **Der Benutzer darf die Firewall ein- und ausschalten** und **Firewall** > **Übersicht** > **Der Benutzer darf die Offsite-Konfiguration ändern**).



- **Sicherheit**: Firewall aktivieren oder deaktivieren.
- **Modus**: Die Firewall kann mit automatischer (Autopilot) oder manueller Regelerstellung betrieben werden.

8. G Data MailSecurity MailGateway

G Data MailSecurity MailGateway ist das Softwarepaket zum Komplettschutz Ihrer E-Mail-Kommunikation. Neben der eigentlichen Software, die im Hintergrund läuft, wurde automatisch der **MailSecurity Administrator** installiert, über den Sie vollen Zugriff auf die Funktionen und Optionen des MailGateways haben. Diesen Administrator finden Sie bei einer Standardinstallation unter **Start** > **Programme** > **G Data MailSecurity** > **G Data MailSecurity**. Wenn Sie die Administrator-Software beenden, schließen Sie damit nicht das MailGateway. Dieses bleibt weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen eingestellt wurden.

Sie können das MailGateway auch über jeden anderen Rechner warten, der die Systemvoraussetzungen für das G Data MailSecurity Administrator-Tool erfüllt. Wenn Sie das MailGateway also über einen anderen Rechner im Netzwerk ansteuern möchten, installieren Sie dort einfach den Administrator ohne die eigentliche MailGateway-Software. Starten Sie dazu einfach erneut das Setup und wählen die Schaltfläche **G Data MailSecurity Administrator** aus.

9. G Data MailSecurity Administrator

Der G Data MailSecurity Administrator ist die Steuerungssoftware für das G Data MailSecurity MailGateway, das - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr mit und in Ihrem gesamten Netzwerk sichert. Der Administrator kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Einstellungsänderungen am Virenscanner und Virensignatur-Updates möglich.

9.1. Starten des G Data MailSecurity Administrators

Sie können das AdministratorTool zur Steuerung des MailGateways mit einem Klick auf den Eintrag G Data MailSecurity in der Programmgruppe **Start** > **(Alle) Programme** > **G Data MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem **Server** und dem **Kennwort** gefragt. Geben Sie in dem Feld Server, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde.

Beim ersten Login haben Sie noch kein Kennwort vergeben. Klicken Sie ohne Eingabe eines Kennworts auf die **OK**-Schaltfläche. Es öffnet sich ein Kennworteingabefenster, in dem Sie unter **Neues Kennwort** ein neues Kennwort für den G Data MailSecurity Administrator vergeben können. Sie bestätigen das eingegebenen Kennwort durch erneutes Eintippen im Feld **Neues Kennwort bestätigen** und klicken dann auf **OK**. Sie können das Kennwort jederzeit im Bereich **Optionen** in der Karteikarte **Erweitert** mit einem Klick auf die Schaltfläche **Kennwort ändern** neu vergeben.

9.2. G Data MailSecurity Administrator konfigurieren

Die Menüleiste des G Data MailSecurity Administrators bietet Ihnen folgende Optionen:

Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb Ihrer G Data MailSecurity verändern und an individuelle Bedürfnisse anpassen.

Update: Im Internet Update-Bereich können Sie grundlegende Einstellungen zum automatischen Download von aktuellen Virensignaturen aus dem Internet vornehmen. Sie können die Zeitplanungen für diese Downloads individuellen Bedürfnissen anpassen und außerdem Updates der Programmdateien von G Data MailSecurity durchführen.

Spam-Filter: Die Schaltfläche Spam-Filter ist eine Verknüpfung zu den Spam-Filter-Einstellungen im **Filter**-Modul.

Hilfe: Hier rufen Sie die Online-Hilfe zum Produkt auf.

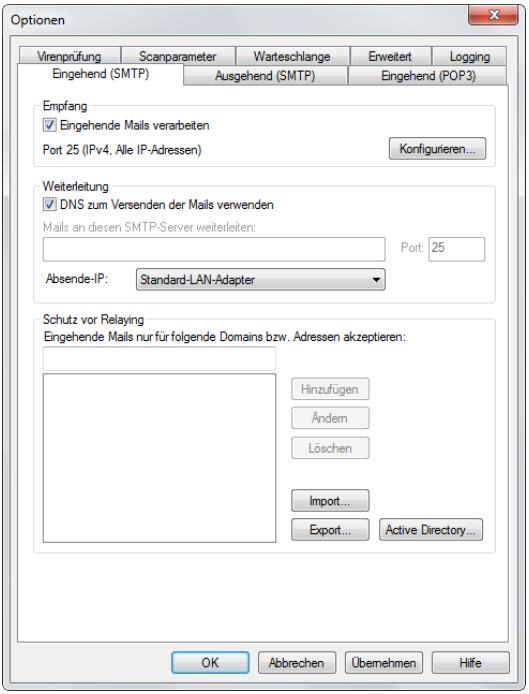
Info: Hier erhalten Sie Informationen zur Programmversion.

9.2.1. Optionen

Im Optionen-Bereich können Sie umfangreiche Einstellungen vornehmen, um G Data MailSecurity optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Dazu stehen Ihnen verschiedene thematisch untergliederte Einstellungsbereiche in verschiedenen Karteikarten zur Verfügung, die Sie durch Anklicken des jeweiligen Karteireiters in den Vordergrund holen.

9.2.1.1. Eingehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

Hier können Sie festlegen, ob eingehende Mails verarbeitet werden sollen. Generell ist hier Port 25 voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

Zur Weiterleitung der eingehenden Mails an Ihren Mail-Server deaktivieren Sie bitte die Option **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** den gewünschten Server an. Geben Sie bitte auch den **Port** an, über den die Mails an den SMTP-Server weitergeleitet werden sollen. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Schutz vor Relaying

Um einen Missbrauch Ihres Mail-Servers zu unterbinden, können und sollten Sie unter **Eingehende Mails nur für folgende Domains bzw. Adressen akzeptieren** die Domains festlegen, an die SMTP-Mails versendet werden dürfen. Auf diese Weise kann Ihr Server nicht zur Weiterleitung von SPAM-Mails an andere Domains missbraucht werden.

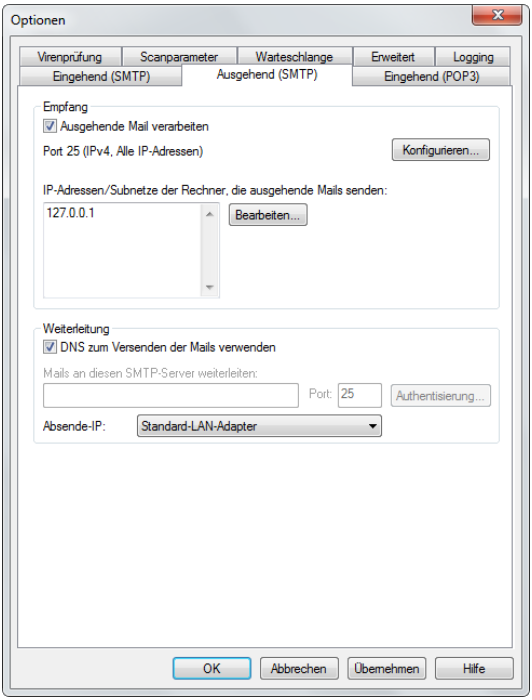
Achtung: Wenn Sie hier keine Domains eintragen, werden auch keine Mails

angenommen. Sollen alle Mails von allen Domains angenommen werden, muss hier ein *.* (Sternchen Punkt Sternchen) hinzugefügt werden.

Der Relay-Schutz kann wahlweise auch über eine Liste von gültigen E-Mail-Adressen realisiert werden. Mails für Empfänger, die nicht auf der Liste stehen, werden nicht angenommen. Um die Pflege dieser Mailadressen zu automatisieren, können diese automatisch und periodisch aus dem **Active Directory** gelesen werden. Für die Active Directory-Anbindung wird mindestens das .NET Framework 1.1 benötigt.

9.2.1.2. Ausgehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle ausgehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

Über das Häkchenfeld **Ausgehende Mail verarbeiten** legen Sie fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **IP-Adressen/Subnetze der Rechner, die ausgehende Mails senden** können Sie bestimmen, von welchen IP-Adressen die zu überprüfenden Mails kommen. Wenn mehrere IP-Adressen dafür in Frage kommen, trennen Sie bitte die einzelnen IP-Adressen durch ein Komma voneinander ab. Diese Eingabe ist nötig, damit das MailGateway eingehende und ausgehende Mails voneinander unterscheiden kann.

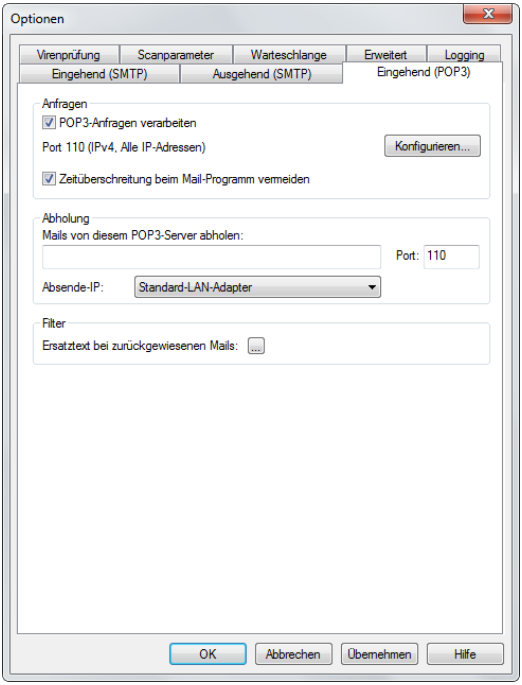
Generell ist der Port 25 für den Empfang ausgehender Mails voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Einstellungen für eingehende Mails definieren.

Weiterleitung

Aktivieren Sie den Eintrag **DNS zum Versenden der Mails verwenden**, damit die Mails direkt an den für die Zieldomäne zuständigen Mail-Server geschickt werden. Wenn Sie die Mails indirekt über ein Relay (z.B. einen Provider) versenden möchten, deaktivieren Sie DNS zum Versenden der Mails verwenden und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** das Relay an. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

9.2.1.3. Eingehend (POP3)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender POP3-Mails auf Ihrem Mail-Server vorzunehmen.



Anfragen

Unter **POP3-Anfragen verarbeiten** aktivieren Sie die Möglichkeit, über G Data MailSecurity Ihre POP3-Mails vom entsprechenden POP3-Server abzuholen, auf Viren

zu überprüfen und über Ihren Mail-Server an die Empfänger weiterzuleiten. Sie müssen dazu gegebenenfalls den **Port** angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel Port 110). Mit der Funktion **Zeitüberschreitung beim Mail-Programm vermeiden** überbrücken Sie die Zeit, die G Data MailSecurity zum Überprüfen der E-Mails benötigt und verhindern so, dass der Empfänger beim Abruf seiner POP3-Mails möglicherweise vom Mail-Programm einen Timeout-Fehler enthält, weil die Daten nicht sofort zur Verfügung stehen (sondern je nach Mail-Aufkommen erst ein paar Sekunden verzögert).

POP3-basierte Mailprogramme können manuell konfiguriert werden. Verwenden Sie dabei in Ihrem Mail-Programm 127.0.0.1 bzw. den Server Ihres MailGateways als eingehenden POP3-Server und schreiben Sie den Namen des externen Mail-Servers, mit einem Doppelpunkt getrennt, vor den Benutzernamen. Also z.B. statt *POP3-Server:mail.xxx.de/Benutzername:Erika Musterfrau* schreiben Sie *POP3-Server:127.0.0.1/Benutzername:mail.xxx.de:Erika Musterfrau*. Um eine manuelle Konfiguration durchzuführen, informieren Sie sich bitte auch in der Bedienungsanleitung Ihres Mail-Programms über die notwendigen Schritte für eine manuelle Konfiguration.

Abholung

Unter **Mails von diesem POP3-Server abholen** müssen Sie gegebenenfalls den POP3-Server angeben, von dem Sie die Mails abholen (z.B. *pop3.maildienstanbieter.de*).

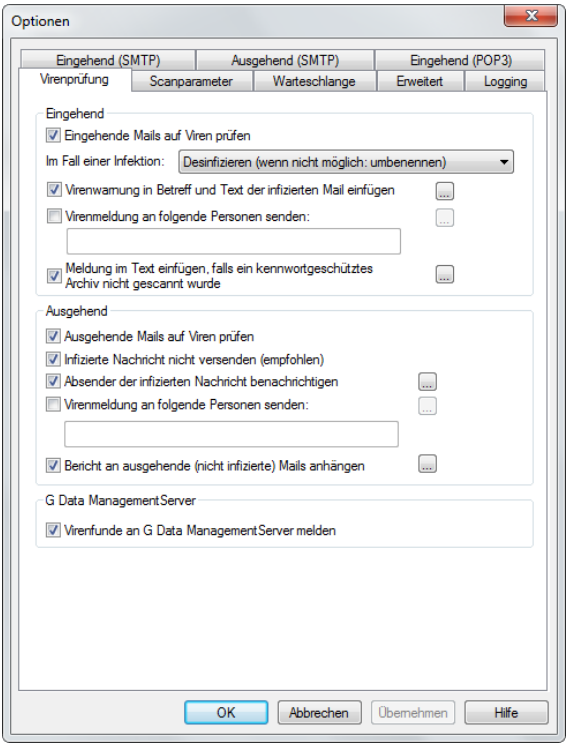
Filter

Wenn POP3-Mails auf Grund einer Content-Prüfung oder auf Grund eines Virenbefalls zurückgewiesen werden, kann der Absender dieser Nachricht automatisch darüber informiert werden. Der Ersatztext bei zurückgewiesenen Mails lautet dabei: *Die Nachricht wurde vom Systemadministrator zurückgewiesen*. Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v > Virus
- %s > Absender
- %r > Empfänger
- %c > Cc
- %d > Datum
- %u > Betreff
- %h > Header
- %i > Absender-IP

9.2.1.4. Virenprüfung

Bei der Virenprüfung haben Sie die Möglichkeit, Virenprüfungsoptionen für ein- und ausgehende Mails einzustellen.



Eingehend

Grundsätzlich sollten Sie natürlich die Funktion **Eingehende Mails auf Viren prüfen** aktiviert haben und auch darauf achten, welche Option Sie **Im Fall einer Infektion** nutzen möchten.

- **Nur protokollieren**
- **Desinfizieren (wenn nicht möglich: nur protokollieren)**
- **Desinfizieren (wenn nicht möglich: umbenennen)**
- **Desinfizieren (wenn nicht möglich: löschen)**
- **Infizierte Anhänge umbenennen**
- **Infizierte Anhänge löschen**
- **Nachricht löschen**

Optionen, in denen nur ein Protokollieren eingehender Viren stattfindet, sollten Sie nur dann verwenden, wenn Sie Ihr System auf andere Weise permanent vor Virenbefall geschützt haben (z.B. mit dem Client/Server-basierten Virenschutz G Data AntiVirus).

Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie eine Virenwarnung in Betreff und Text der infizierten Mail einfügen, um den Empfänger einer solchen Mail zu informieren. Auch können Sie eine Meldung über den Virenfund an bestimmte Personen senden, also z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass ein Virus an eine E-Mail-Adresse in ihrem Netzwerk verschickt wurde. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

Ausgehend

Grundsätzlich sollten Sie die Funktion **Ausgehende Mails auf Viren prüfen** aktiviert haben und die Funktion **Infizierte Nachricht nicht versenden** standardmäßig eingeschaltet haben. Auf diese Weise verlässt kein Virus Ihr Netzwerk und richtet möglicherweise bei Geschäftspartnern Schaden an. Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie den **Absender der infizierten Nachricht benachrichtigen** und unter **Virenmeldung an folgende Personen senden** z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass aus Ihrem Netzwerk ein Virus verschickt werden sollte. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Klicken Sie dazu einfach auf die **...**-Schaltfläche rechts. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

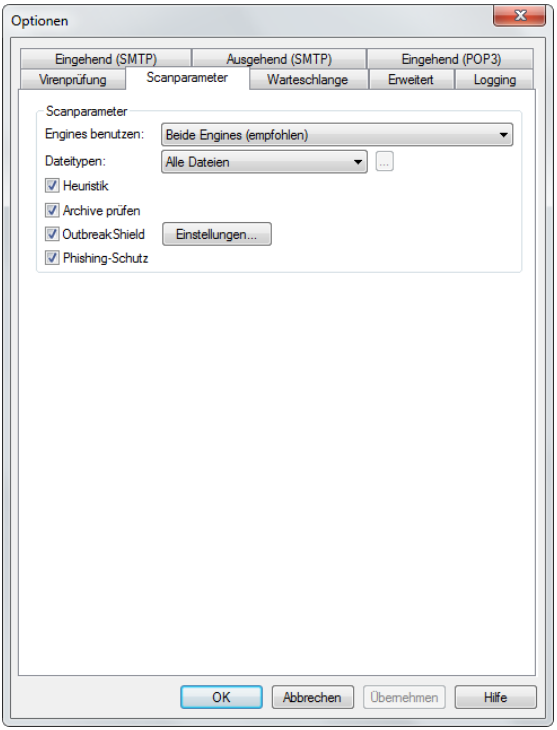
Zusätzlich haben Sie unter **Bericht an ausgehende (nicht infizierte) Mails anhängen** die Möglichkeit, von G Data MailSecurity geprüfte Mails mit einem Bericht am Ende des Mailtextes zu versehen, in dem explizit darauf hingewiesen wird, dass diese Mail von G Data MailSecurity geprüft wurde. Selbstverständlich können Sie diesen Bericht aber auch individuell verändern oder ganz weglassen.

G Data ManagementServer

Wenn Sie den Client/Server-basierten Virenschutz G Data AntiVirus (z.B. im Rahmen der G Data AntiVirus-Lösung) installiert haben, können Sie über das Setzen des Häkchens bei **Virenfunde an G Data ManagementServer melden** dafür sorgen, dass der G Data ManagementServer über Virenfunde des MailGateways benachrichtigt wird und Ihnen auf diese Weise einen umfassenden Überblick über die Virenbelastung bzw. -gefährdung Ihres Netzwerkes liefert.

9.2.1.5. Scanparameter

In diesem Bereich können Sie die Virenerkennungsleistung von G Data MailSecurity optimieren und an persönliche Erfordernisse anpassen. Generell gilt, dass durch eine Verringerung der Virenerkennungsleistung die Performance des Gesamtsystems steigt, während eine Erhöhung der Virenerkennungsleistung möglicherweise leichte Einbußen in der Performance mit sich bringen kann. Hier ist von Fall zu Fall abzuwägen.



Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen**: G Data MailSecurity arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Unter Engines benutzen stellen Sie ein, wie diese miteinander kooperieren. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.
- **Dateitypen**: Unter Dateitypen können Sie festlegen, welche Dateitypen von G Data MailSecurity auf Viren untersucht werden sollen. Wir empfehlen hier die automatische Typ-Erkennung über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Wenn Sie selber die Dateitypen definieren möchten, für die eine Virenprüfung erfolgen soll,

verwenden Sie die Funktion **Benutzerdefiniert**. Durch Anklicken der **...**-Schaltfläche können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über die **Hinzufügen**-Schaltfläche in die Liste der benutzerdefinierten Dateitypen übernehmen. Sie können dabei auch mit Platzhaltern arbeiten.

Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen. Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen. Um z.B. sämtliche Dateien mit der Dateiendung exe prüfen zu lassen, geben Sie also **.exe* ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. xlr, xls), geben Sie einfach **.xl?* ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise *text*.** ein.

- **Heuristik**: In der Heuristik-Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann sie in seltenen Fällen auch einen Fehlalarm erzeugen.
- **Archive prüfen**: Das Überprüfen gepackter Dateien in Archiven sollten generell aktiviert sein.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht. Wenn Sie OutbreakShield verwenden möchten, geben Sie über die Schaltfläche **Einstellungen** an, ob Sie einen Proxyserver verwenden und gegebenenfalls - um OutbreakShield einen jederzeitigen Zugang zum Internet zu ermöglichen - die **Zugangsdaten für die Internetverbindung**. Auf der Registerkarte OutbreakShield können Sie den Text der Mail definieren, den ein Mailempfänger enthält, wenn eine an ihn gerichtete Massenmail zurückgewiesen wurde.

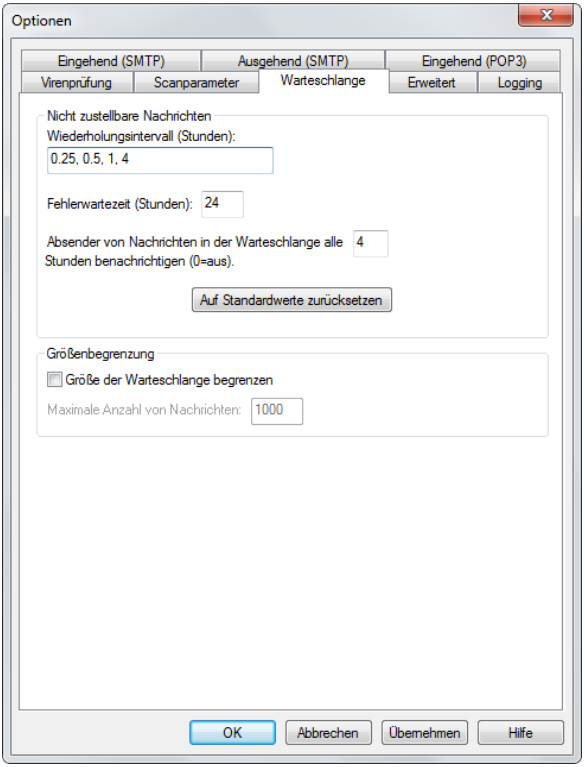
  Da das OutbreakShield auf Grund seiner eigenständigen Architektur infizierte Mailanhänge nicht desinfizieren, umbenennen oder in die Quarantäne verschieben kann, informiert der Ersatztext den Anwender darüber, dass ihm die verdächtige bzw. infizierte Mail nicht zugestellt wurde. Eine Meldung über vom OutbreakShield zurückgewiesene Mails entfällt, wenn Sie auf der Karteikarte **Virenprüfung** > **Eingehend** unter **Im Falle einer Infektion** den Punkt **Nachricht löschen** auswählen. In diesem Fall werden alle infizierten Mails, inklusive derer, die ausschließlich vom OutbreakShield erkannt werden, direkt gelöscht.

- **Phishing-Schutz**: Aktivieren Sie den Phishing-Schutz, um E-Mails von vermeintlich seriösen Institutionen zu blockieren. Diese sogenannten Phishing-Mails werden versendet, um Benutzerdaten wie z.B. Kennwörter, Kreditkarteninformationen oder andere persönlichen Daten von Ihrem Rechner zu sammeln.

9.2.1.6. Warteschlange

In diesem Bereich können Sie festlegen, wie oft und in welchen Abständen der erneute Versand von Mails erfolgen soll, die vom MailGateway nicht an den entsprechenden Mail-Server weitergeleitet werden können.

Generell gelangen Mails erst nach der Virenüberprüfung durch G Data MailSecurity in die Warteschlange. Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z.B. der Mail-Server, an den Sie nach der Virenprüfung weitergeleitet werden sollen, überlastet oder ausgefallen sein.



Nicht zustellbare Nachrichten

Geben Sie unter **Wiederholungsintervall** an, in welchen Abständen G Data MailSecurity einen neuen Versendeversuch unternehmen soll. So bedeutet z.B. die Angabe *1, 1, 1, 4*, dass G Data MailSecurity die ersten drei Stunden stündlich versucht, die Mail zu verschicken und von da an regelmäßig im Abstand von 4 Stunden. Unter **Fehlerwartezeit** legen Sie fest, wann die Versendung der Mail endgültig abgebrochen und die Mail gelöscht wird.

Sie können **Absender von Nachrichten in der Warteschlange alle ... Stunden**

benachrichtigen, wobei ... ein ganzzahliger Stundenwert sein muss. Wenn Sie die Absender einer nicht zustellbaren Nachricht nicht regelmäßig informieren möchten, geben Sie hier einfach eine *0* ein. Auch wenn Sie die regelmäßige Benachrichtigung von Absendern nicht weitergeleiteter Mails abschalten, wird der Absender natürlich dennoch informiert, wenn seine Mail endgültig nicht zugestellt und vom Server gelöscht wurde.

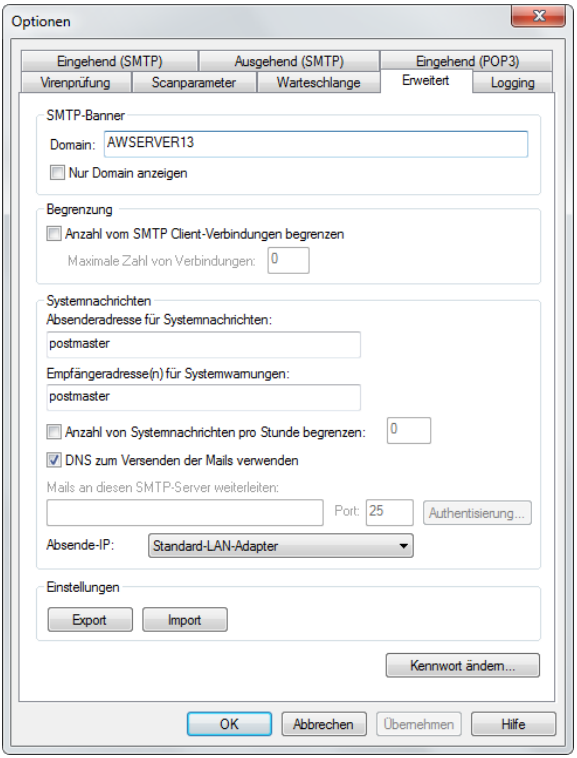
Über die Schaltfläche **Auf Standardwerte zurücksetzen** können Sie die Standardeinstellungen im Bereich Warteschlange wiederherstellen. Diese Einstellungen haben sich in der Praxis bewährt.

Größenbegrenzung

Die Größe der Warteschlange kann auf Wunsch begrenzt werden. Dies dient dem Schutz vor Denial of Service-Attacken. Sollte die Größenbeschränkung überschritten werden, werden keine weiteren Mails mehr in die Warteschlange aufgenommen.

9.2.1.7. Erweitert

Im Erweitert-Bereich können Sie globale Einstellungen von G Data MailSecurity verändern.



SMTP-Banner

Standardmäßig beinhalt das Feld **Domain** den Computernamen. Beim Senden von ausgehenden Mails über DNS sollte der Fully Qualified Domain Name (FQDN) hier eingetragen werden um Reverse-Lookups zu ermöglichen. Aktivieren Sie **Nur Domain anzeigen**, um die Anzeige der Server-Version in der Kommunikation mit anderen Servern zu unterdrücken.

Begrenzung

Um die Anzahl der SMTP-Verbindungen zu begrenzen, die G Data MailSecurity gleichzeitig verarbeitet, setzen Sie bitte das Häkchen vor **Anzahl von SMTP Client-Verbindungen begrenzen**. G Data MailSecurity lässt dann nur die maximale Zahl von Verbindungen zu, die Sie vorgeben. Auf diese Weise können Sie die Mailfilterung an die Leistung der Hardware anpassen, die Sie für das MailGateway verwenden.

Systemnachrichten

Die **Absenderadresse für Systemnachrichten** ist die Mail-Adresse, die z.B. dazu verwendet wird, Absender und Empfänger vireninfizierter Mails zu informieren oder darüber zu informieren, dass sich ihre Mails in der Warteschlange befinden. G Data MailSecurity Systemwarnungen sind unabhängig von den allgemeinen Mitteilungen bei Virenfunden. Bei einer Systemwarnung handelt es sich in der Regel um eher globale Informationen, die nicht mit einer einzelnen möglicherweise infizierten Mail in Zusammenhang stehen. So würde G Data MailSecurity z.B. eine Systemwarnung verschicken, wenn die Virenkontrolle aus irgendwelchen Gründen nicht mehr gewährleistet ist.

Einstellungen

Über die Schaltflächen **Import** und **Export** können Sie die Einstellungen der Programm-Optionen auch als XML-Datei speichern und so ggf. erneut einspielen, wenn der Bedarf gegeben ist.

Kennwort ändern

Hier können Sie das Administrator-Passwort ändern, dass Sie beim ersten Start von G Data MailSecurity vergeben haben. Geben Sie dazu einfach das momentan aktuelle Passwort unter **Altes Kennwort** ein und dann unter **Neues Kennwort** und **Neues Kennwort bestätigen** das neue Kennwort. Mit Anklicken der **OK**-Schaltfläche wird die Kennwortänderung durchgeführt.

9.2.1.8. Logging

Im Logging-Bereich können Sie den Mailverkehr auf Ihrem Server statistisch auswerten. Die Ergebnisse dieser Statistikfunktion können Sie im Statistik-Bereich der Programmoberfläche aufrufen, den Sie durch Anklicken der Schaltfläche **Statistik** im Programmbereich **Status** finden. Alternativ können Sie die ermittelten Daten auch in einer externen Log-Datei abspeichern (maillog.txt, gespeichert in MailSecurity's Installationsverzeichnis). Über die Funktionen **Nur Junk-Mails** und **Anzahl von E-**

Mails begrenzen können Sie die Größe dieser Log-Datei gegebenenfalls begrenzen.

9.2.2. Update

Im Update-Bereich können Sie umfangreiche Einstellungen vornehmen, um G Data MailSecurity optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Hier können Sie die Virensignaturen und Programmdaten von G Data MailSecurity manuell oder automatisiert auf den neuesten Stand bringen.

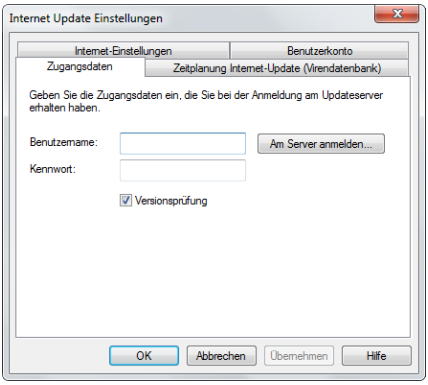
9.2.2.1. Einstellungen

Hier können Sie grundlegende Einstellungen für das Internet Update vorgeben. Wenn Sie (z.B. im Rahmen der G Data AntiVirus-Lösung) parallel zu G Data MailSecurity das Client/Server-basierte G Data AntiVirus verwenden, können Sie sich über **Virensignaturen vom G Data Security Client verwenden** den doppelten Download der Virensignaturen sparen und diese direkt vom installierten G Data Security Client aus erhalten. Über **Internet Update der Virensignaturen selbst durchführen** führt G Data MailSecurity diesen Vorgang selbstständig durch. Über die Schaltfläche **Einstellungen und Zeitplanung** gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Zugangsdaten

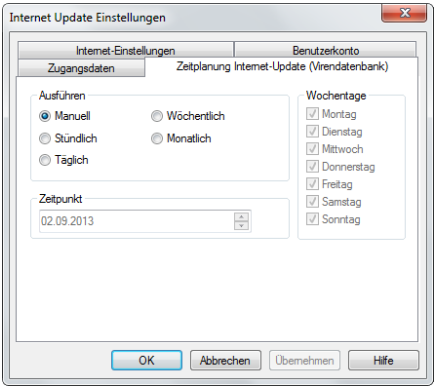
Geben Sie unter Zugangsdaten den **Benutzernamen** und das **Kennwort** ein, das Sie bei der Anmeldung von G Data MailSecurity erhalten haben. Mit Hilfe dieser Daten werden Sie vom G Data-Server erkannt und das Update der Virensignaturen kann

vollautomatisch erfolgen. Klicken Sie auf die Schaltfläche **Am Server anmelden**, wenn Sie sich noch nicht am G Data-Server angemeldet haben. Geben Sie einfach die Anmeldenummer ein (Sie finden diese auf der Rückseite des Benutzerhandbuches), Ihre Kundendaten und klicken Sie auf **Anmelden**. Sofort werden Ihnen die Zugangsdaten (Benutzername und Passwort) angezeigt. Sie sollten sich diese Daten aufschreiben und diese sicher verwahren. Für die Anmeldung am Server ist natürlich (wie auch für das Internet Update der Virensignaturen) eine Internetverbindung notwendig.



Zeitplanung Internet-Update (Virendatenbank)

Über die Karteikarte Zeitplanung Internet-Update (Virendatenbank) können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** spezifizieren.

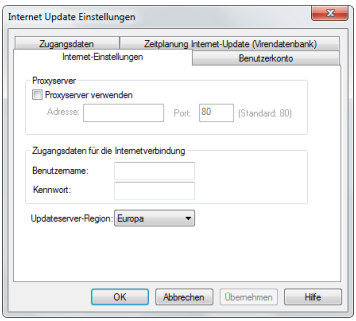


Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter **Zeitpunkt** Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und

nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.

Internet-Einstellungen

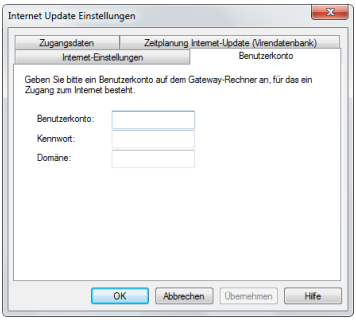
Falls Sie einen Rechner hinter einer Firewall verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet Update nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Internetzugangsanbieter.



Die Zugangsdaten für die Internetverbindung (Benutzernamen und Passwort) sind gerade beim automatischen Internet Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z.B. für Ihr Mailprogramm oder Ihren Internetbrowser) die automatische Einwahl ermöglichen. Ohne die automatische Einwahl startet G Data MailSecurity zwar den Internet Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit **OK** bestätigen. Über die Auswahl unter **Updateserver-Region** können Sie einen Updateserver in Ihrer Region auswählen, um ggf. die Datenübermittlung zu optimieren.

Benutzerkonto

Geben Sie bitte unter **Benutzerkonto** ein Benutzerkonto auf dem MailGateway-Rechner an, für das ein Zugang zum Internet besteht.



Achtung: Bitte verwechseln Sie nicht die Angaben, die Sie in den Karteikarten **Zugangsdaten** und **Benutzerkonto** tätigen.

9.2.2.2. Virensignaturen

Über die Schaltflächen **Virendatenbank aktualisieren** und **Status aktualisieren** können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen haben, ein aktuelles Virensignaturupdate starten.

9.2.2.3. Programmdateien

Über die Schaltfläche **Programm-Update** können Sie auch die Programmdateien von G Data MailSecurity aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

9.3. Programmbereiche

Die Bedienung von G Data MailSecurity ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die im G Data MailSecurity Administrator angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.

9.3.1. Status

Im Status-Bereich des Administrators erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und des MailGateways. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

Solange Ihre G Data MailSecurity optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Ampelsymbol.

Sollte eine Komponente nicht optimal eingestellt sein (z.B. veraltete Virensignaturen, abgeschaltete Virenprüfung), weist Sie ein Achtung-Symbol darauf hin.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken der **Bearbeiten**-Schaltfläche) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol. Folgende Einträge stehen Ihnen zur Verfügung:

- **Verarbeitung eingehender Mail**: Die Verarbeitung eingehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Eingehend (SMTP)** und **Optionen** > **Eingehend (POP3)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung eingehender Mail**: Die Prüfung eingehender Mails verhindert, dass infizierte Dateien in Ihr Netz gelangen. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Verarbeitung ausgehender Mail**: Die Verarbeitung ausgehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Ausgehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung ausgehender Mail**: Die Prüfung ausgehender Mails verhindert, dass aus Ihrem Netz infizierte Dateien verschickt werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung ausgehender Mails an individuelle Bedürfnisse anpassen.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht.
- **Automatische Updates**: Die Virensignaturen können selbstständig aktualisiert werden. Sie sollten die Option für automatische Updates generell aktiviert haben. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie

in das dazugehörige Einstellungsfenster (Menüleiste: **Update**) und können die Updatefrequenz an individuelle Bedürfnisse anpassen.

- **Datum der Virensignaturen**: Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten und diesen Prozess möglichst automatisieren. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Update**) und können auch direkt ein Internet Update (unabhängig von etwaigen Zeitplänen) durchführen.
- **Spam-Filter**: Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.
- **Spam-OutbreakShield**: Mit dem Spam-OutbreakShield können Massenmails schnell und sicher erkannt und bekämpft werden. Das Spam-OutbreakShield erfragt dabei vor dem Abruf von Mails über das Internet besondere Häufungen von verdächtigen Mails ab und lässt diese gar nicht erst in das Postfach des Empfängers gelangen.

Wenn Sie bei der Installation die Option E-Mail-Statistik aktiviert haben, können Sie über die Schaltfläche **Statistik** Zugriff auf die statistische Auswertung Ihres Mailverkehrs bzw. Spamaufkommens nehmen. Das Konfigurieren der Statistik erfolgt dabei im **Optionen**-Menü des Administrators auf der Registerkarte namens **Logging**.

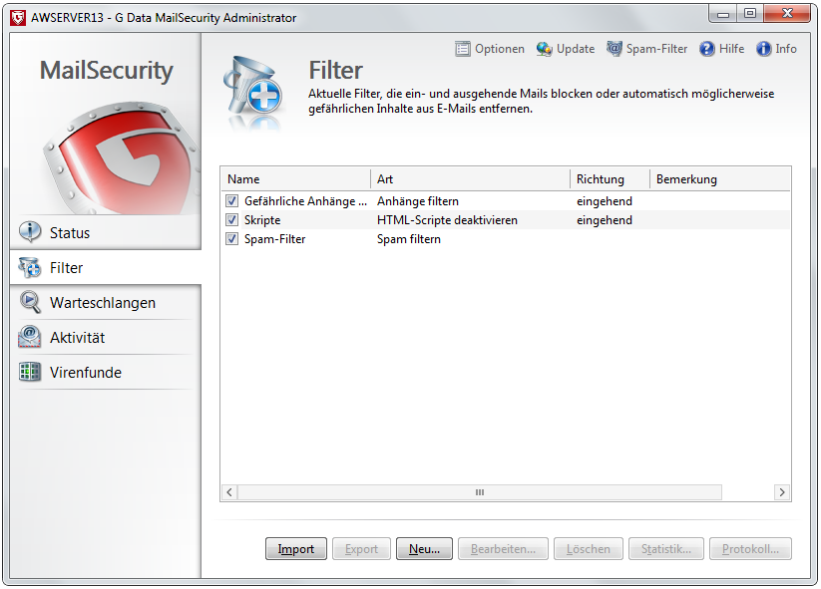
9.3.2. Filter

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende Mails blocken oder automatisch möglicherweise gefährliche Inhalte aus Mails entfernen. Die jeweiligen Filter werden in der Liste im Filter-Bereich angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden.

- **Import**: Sie können einzelne Filter mit ihren speziellen Einstellungen aus XML-Dateien importieren.
- **Export**: Sie können einzelne Filter mit ihren speziellen Einstellungen als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen. Um mehrere Filter zu exportieren, wählen Sie diese bitte mit der Maus aus und halten dabei die Strg-Taste gedrückt.
- **Neu**: Über die Neu-Schaltfläche können Sie neue Filterregeln anlegen. Wenn Sie einen neuen Filter anlegen, öffnet sich ein Auswahlfenster, in dem Sie den grundlegenden Filtertyp festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten Assistentenfenster angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.
- **Bearbeiten**: Über die Bearbeiten-Schaltfläche können Sie vorhandene Filter bearbeiten.

- **Löschen**: Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann die Löschen-Schaltfläche.
- **Statistik**: Zu jedem Filter können Sie statistische Informationen aufrufen.
- **Protokoll**: Für den Spam-Filter gibt es ein Protokoll mit einer Liste, in der die als Spam eingestuften Mails aufgelistet sind. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (Spam-Index-Werte). Hier können Sie ggf. bei einer fälschlichen Einstufung einer Mail als Spam den OutbreakShield-Server online darüber informieren, dass hier eine Fehlkennung (False Positive) vorliegt. Die Mail wird dann vom OutbreakShield erneut geprüft und - falls sie tatsächlich fälschlicherweise als Spam erkannt wurde - des Weiteren als unbedenklich eingestuft. Hierbei wird lediglich eine Prüfsumme übermittelt und nicht der Inhalt dieser Mail.

Selbstverständlich ist Ihr Netzwerk auch unabhängig von individuellen Filterregeln vor Virenbefall geschützt, da G Data MailSecurity ständig im Hintergrund eingehende und ausgehende Mails überprüft. Filterregeln dienen eher dazu, Ihre E-Mail-Accounts vor unerwünschten Mails, Spam und unsicheren Skripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch G Data MailSecurity zu minimieren.

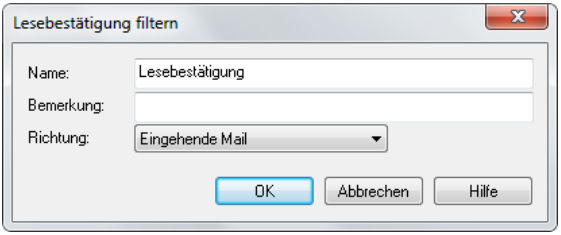


Generell können Sie bei allen Filtertypen unter **Name** einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter **Bemerkung** interne Bemerkungen und Notizen zu dem betreffenden Filter angeben. Unter **Richtung** können Sie generell bestimmen, ob eine Filterregel nur für **Eingehende Mails**, nur für **Ausgehende Mails** oder **Beide Richtungen** gelten soll.

Im Abschnitt **Reaktion** können Sie festlegen, wie mit Mails verfahren werden soll, sobald sie die Filterkriterien erfüllen, also als Spam-Mails definiert wurden. Sie können dabei den Text für die Funktionen **Absender der Nachricht benachrichtigen** und **Meldung an folgende Personen senden** individuell gestalten. Klicken Sie dazu einfach auf die Schaltfläche rechts von der jeweiligen Reaktion. Wildcards können verwendet werden, um Informationen in den **Betreff**- und **Mailtext**-Feldern einzufügen. Hierbei handelt es sich um die gleichen Platzhalter, wie diejenigen, die unter **Eingehend (POP3)** > **Filter** verwendet werden.

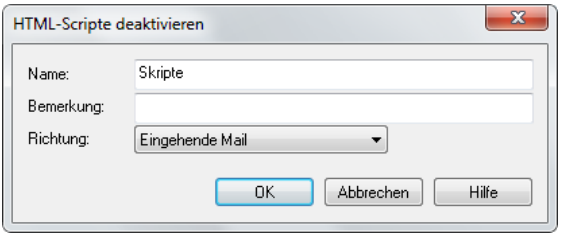
9.3.2.1. Lesebestätigung filtern

Dieser Filter löscht Lesebestätigungs-Anfragen für eingehende oder ausgehende E-Mails.



9.3.2.2. HTML-Scripte deaktivieren

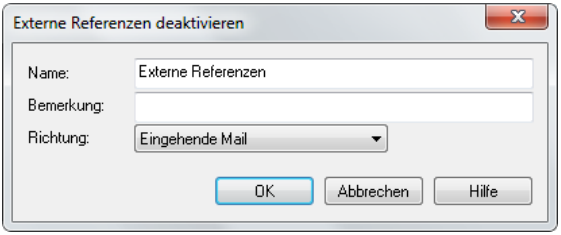
Dieser Filter deaktiviert Skripte im HTML-Teil einer Mail. Skripte, die in einer Internetseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der Vorschauansicht einer Mail wirksam werden können.



9.3.2.3. Externe Referenzen deaktivieren

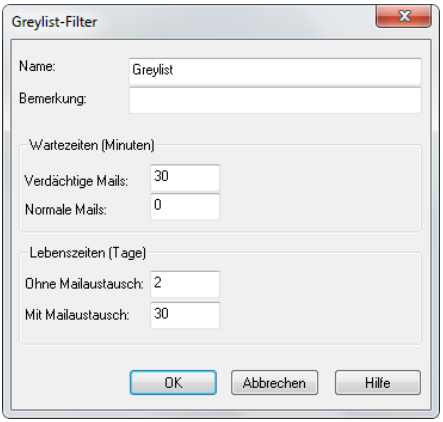
Viele Newsletter und Produktinformationen im HTML-Mailformat beinhalten Links, die erst dann ausgeführt und angezeigt werden, wenn die Mail geöffnet wird. Dies können z.B. Grafiken sein, die nicht mit der Mail versandt wurden, sondern erst über einen Hyperlink automatisch nachgeladen werden. Da es sich hierbei nicht nur um harmlose

Grafiken handeln kann, sondern durchaus auch um Schadroutinen, ist es sinnvoll, diese Referenzen zu deaktivieren. Der eigentliche Mail-Text ist von dieser Deaktivierung nicht betroffen.



9.3.2.4. Greylist-Filter

Greylist-Filter sind eine effektive Methode, um das Spam-Aufkommen zu reduzieren. Hierbei werden E-Mails von unbekannten Absendern nicht sofort beim ersten Zustellversuch über den SMTP-Server an den Mail-Empfänger übermittelt. Da Spam-Versender in der Regel keine Queue-Verwaltung nutzen und ihre Mails selten ein zweites Mal an denselben SMTP-Server schicken, kann die Anzahl an übermittelten Spam-Mails erheblich sinken.



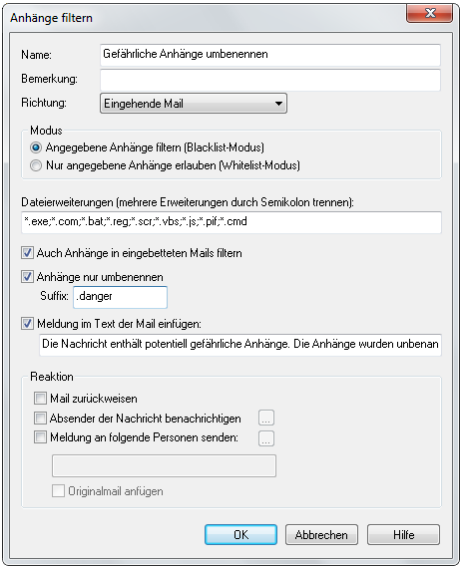
- **Wartezeiten (Minuten)**: Über diese Einstellungen können Sie festlegen, wie lange die Übermittlung verdächtiger Mails blockiert werden soll. Nach Ablauf dieser Zeitspanne wird die Mail bei einem erneuten Sendeversuch dann übermittelt. Wenn der Adressat auf diesen Absender reagiert, wird dieser aus dem Greylist-Filter herausgenommen und in eine Whitelist eingetragen. Nun wird die Zustellung dieser Mails nicht mehr blockiert bzw. verzögert.
- **Lebenszeiten (Tage)**: Damit die Whitelist der erwünschten Absender aktuell bleibt, verbleibt eine Absenderadresse nur eine bestimmte Zeit auf der Whitelist, bevor sie wieder auf Greylist-Status gesetzt wird. Der Timer wird für den jeweiligen Absender bei jedem neuen Mailversand wieder zurückgesetzt.

Wenn Sie hier z.B. einen Wert über 30 Tage eintragen, können Sie auch erwünschte monatliche Newsletter permanent auf der Whitelist führen.

Der Greylist-Filter kann nur dann ausgewählt werden, wenn auch der **Spam-Filter** von G Data MailSecurity aktiviert ist. Außerdem muss eine SQL-Datenbank auf dem Server installiert sein.

9.3.2.5. Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um Mail-Anhänge (Attachments) und Anlagen zu filtern. Die meisten E-Mailviren verbreiten sich über solche Attachments, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische EXE-Datei handeln, die ein Schadprogramm enthält, aber auch um VB-Skripte, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat.



Unter **Dateierweiterungen** können Sie die Dateiendungen aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z.B. alle ausführbaren Dateien (z.B. EXE und COM-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z.B. MPEG, AVI, MP3, JPEG, JPG, GIF etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mail-Server darstellen. Selbstverständlich können Sie auch beliebige Archivdateien (z.B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch Semikolon, z.B. **.exe; *.dll*. Geben Sie

unter Modus an, ob Sie die unter Dateierweiterungen aufgelisteten Dateiendungen erlauben möchten (**Nur angegebene Anhänge erlauben**) oder verbieten (**Angegebene Anhänge filtern**).

Über die Funktion **Auch Anhänge in eingebetteten Mails filtern** sorgen Sie dafür, dass die Filterung der unter Dateierweiterungen ausgewählten Anlagentypen auch in Mails stattfindet, die selber eine Anlage einer Mail darstellen. Diese Option sollte generell aktiviert sein. Über **Anhänge nur umbenennen** werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z.B. bei ausführbaren Dateien (wie z.B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare Skripte und Makros enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbedacht durch einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das Häkchen bei Anhänge nur umbenennen nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht.

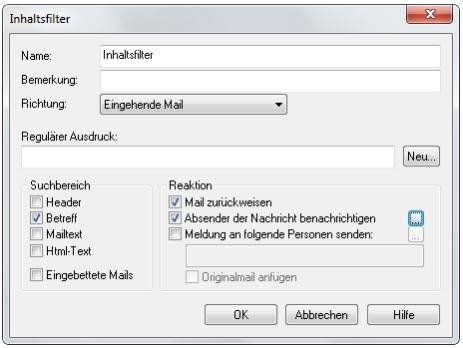
Unter **Suffix** geben Sie die Zeichenfolge ein, mit der Sie die eigentliche Dateiendung erweitern möchten, auf diese Weise wird die Ausführbarkeit einer Datei durch einfaches Anklicken verhindert (z.B. **.exe_danger*). Unter **Meldung im Text der Mail einfügen** können Sie den Empfänger der gefilterten Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

9.3.2.6. Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter **Regulärer Ausdruck** einfach die Schlüsselwörter und Ausdrücke ein, auf die G Data MailSecurity reagieren soll und geben Sie unter **Suchbereich** an, in welchen Bereichen einer Mail nach diesen Ausdrücken gesucht werden soll. Über die **Neu**-Schaltfläche rechts vom Eingabefeld für Regulärer Ausdruck können Sie auf bequeme Weise Text eingeben, der eine Filteraktion hervorruft. Dabei können Sie Text auf beliebige Weise mit den logischen Operatoren UND und ODER verknüpfen.

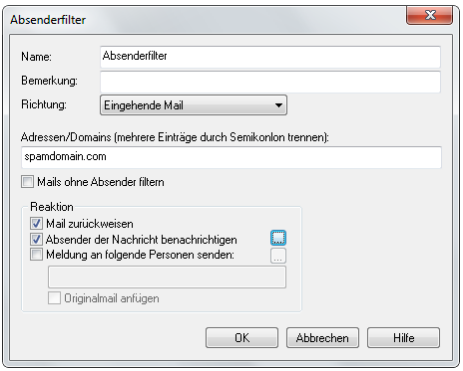
> Wenn Sie z.B. *Alkohol UND Drogen* eingeben, würde der Filter bei einer Mail, die z.B. die Begriffe *Alkohol* und *Drogen* enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff *Alkohol* oder nur den Begriff *Drogen* enthält. Der logische Operator UND setzt also voraus, dass alle mit UND verknüpften Elemente vorhanden sind, der logische Operator ODER setzt lediglich voraus, dass ein Element vorhanden ist.

Sie können auch ohne die Eingabehilfe unter Regulärer Ausdruck beliebige Suchbegriffe miteinander kombinieren. Geben Sie dazu einfach die Suchbegriffe ein und verknüpfen diese mit den logischen Operatoren. Oder entspricht dem Trennstrich | (AltGr + <). Und entspricht dem Kaufmanns-Und & (Shift + 6).



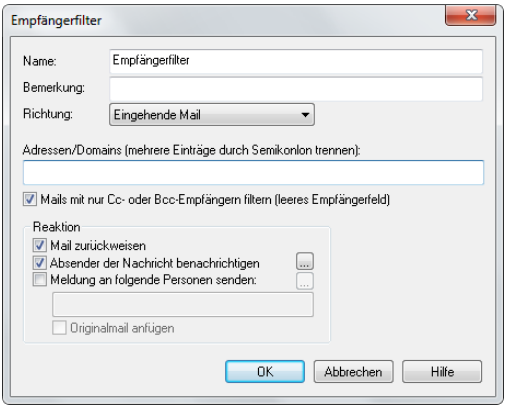
9.3.2.7. Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G Data MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen. Sie können auch Mails ohne Absenderangabe automatisch ausfiltern.



9.3.2.8. Empfängerfilter

Über den Empfängerfilter können Sie E-Mails für bestimmte Empfänger auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G Data MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen. Sie können auch Mails mit leerem Empfängerfeld (also Mails, die nur Bcc- und/oder Cc-Empfänger enthalten) automatisch ausfiltern.



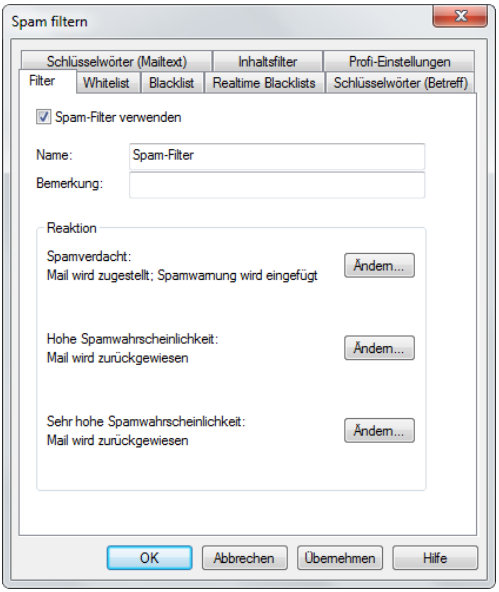
9.3.2.9. Spam filtern

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

Filter

Geben Sie unter **Name** und **Bemerkung** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **Reaktion** können Sie bestimmen, wie der Spam-Filter mit Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch G Data MailSecurity die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

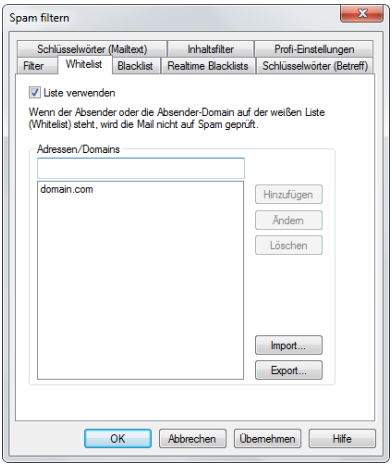
Unter **Spamverdacht** wird der Umgang mit den Mails geregelt, in denen G Data MailSecurity einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um Spam handeln, sondern in seltenen Fällen möglicherweise auch um Newsletter-Mails oder Sammelmailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter **Hohe Spamwahrscheinlichkeit** werden die Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter **Sehr hohe Spamwahrscheinlichkeit** finden sich die Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten Mails ist in den meisten Fällen empfehlenswert. Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten.



So haben Sie über **Mail zurückweisen** die Möglichkeit, die Mail gar nicht erst auf Ihren Mail-Server gelangen zu lassen. Der Empfänger erhält diese Mail dann erst gar nicht. Über **Spamwarnung in Betreff und Text der Mail einfügen** können Sie einen Empfänger einer als Spam identifizierten Mail davon in Kenntnis setzen, dass es sich um Spam handelt. Über die Option **Absender der Nachricht benachrichtigen** können Sie eine automatische Antwortmail an den Absender der als Spam erkannten Mail verschicken, in der Sie diesen darauf hinweisen können, dass seine Mail als Spam erkannt wurde. Da gerade bei Spam viele Mailadressen aber nur einmal verwendet werden, sollten Sie sich überlegen, ob Sie diese Funktion aktivieren. Über die Option **An folgende Personen weiterleiten** können Sie als Spam verdächtige Mails auch automatisch weiterleiten, z.B. an den Systemadministrator.

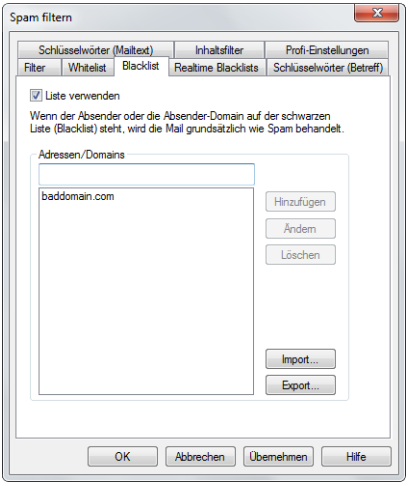
Whitelist

Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Geben Sie dazu einfach in das Feld **Adressen/ Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@gdata.de*) oder Domain (z.B. *gdata.de*) ein, die Sie vom Spamverdacht ausnehmen möchten und G Data MailSecurity behandelt Mails von diesem Absender bzw. dieser Absenderdomain nicht als Spam. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Whitelist auch als Textdatei exportieren.



Blacklist

Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen.

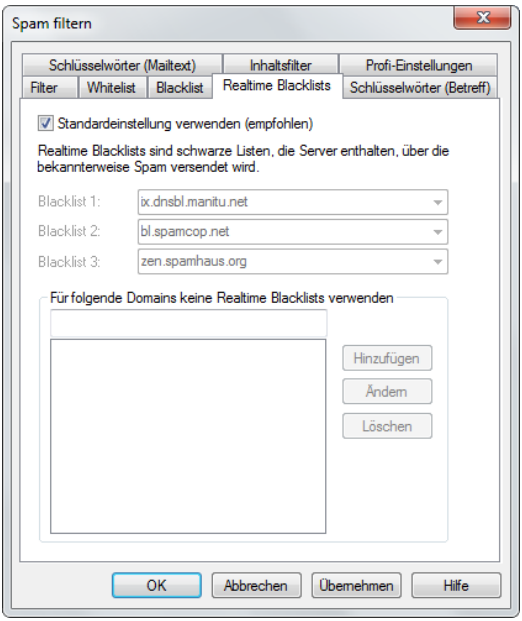


Geben Sie dazu das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@megaspam.de.vu*) oder Domain (z.B. *megaspam.de.vu*) ein, die Sie unter Spamverdacht setzen möchten und G Data MailSecurity behandelt Mails von diesem Absender bzw. dieser Absenderdomain generell als Mails mit sehr hoher Spamwahrscheinlichkeit. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine

solche Blacklist auch als Textdatei exportieren.

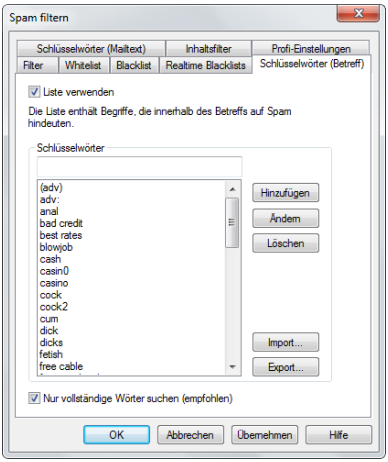
Realtime Blacklists

Im Internet finden sich schwarze Listen, die IP-Adressen von Servern enthalten, über die bekanntermaßen Spam verschickt wird. G Data MailSecurity ermittelt durch DNS-Anfragen an die RBLs (Realtime Blacklists), ob der sendende Server gelistet ist. Falls ja, erhöht sich die Spamwahrscheinlichkeit. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter **Blacklist 1**, **2** und **3** eigene Adressen für Blacklists aus dem Internet vergeben.



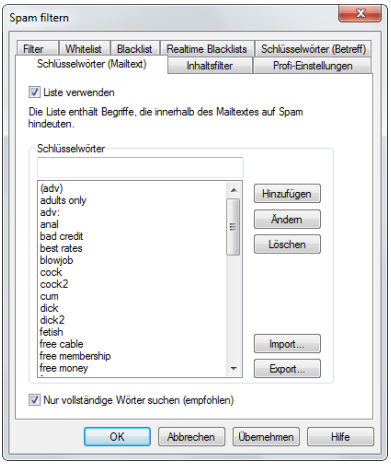
Schlüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der in der Betreffzeile verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G Data MailSecurity die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.



Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der im Mailtext verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe im Mailtext vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern.

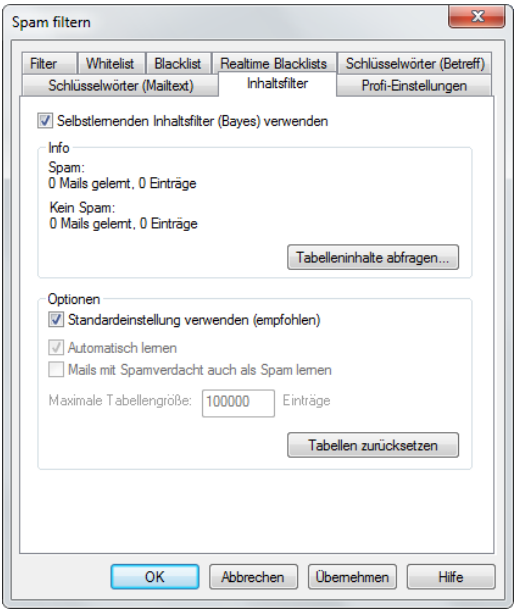


Über die **Import**-Schaltfläche können Sie vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G Data MailSecurity die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht

fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.

Inhaltsfilter

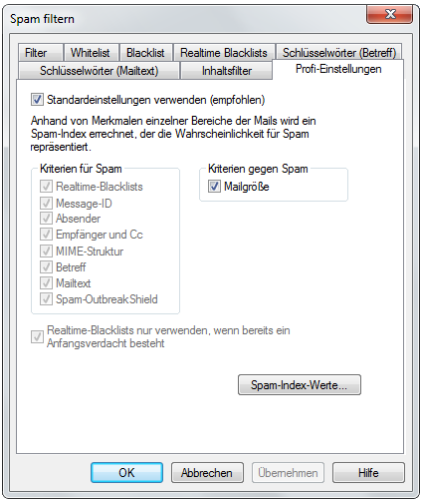
Beim Inhaltsfilter handelt es sich um einen selbstlernenden Filter auf Basis der Bayes-Methode, der auf Grund der im Mailtext verwendeten Worte eine Spamwahrscheinlichkeit berechnet. Dabei arbeitet dieser Filter nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen Mail weiter dazu. Über die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über die Schaltfläche **Tabellen zurücksetzen** löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den Lernvorgang erneut von Beginn an.



Profi-Einstellungen

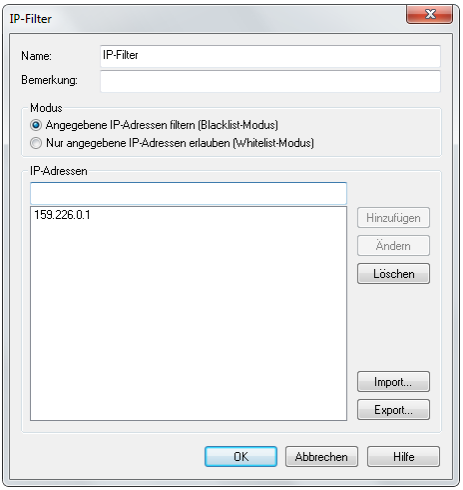
In diesem Bereich können Sie die Spamerkennung von G Data MailSecurity sehr detailliert verändern und an die Gegebenheiten Ihres Mail-Servers anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.

Wählen Sie **Spam-Index-Werte** um die einzelnen Werte zu bearbeiten, die benutzt werden um die Spam-Wahrscheinlichkeit von E-Mails zu klassifizieren. Wir empfehlen hier die Standardwerte.



9.3.2.10. IP-Filter

Der IP-Filter unterbindet den Empfang von Mails, die von bestimmten Servern abgesendet werden.

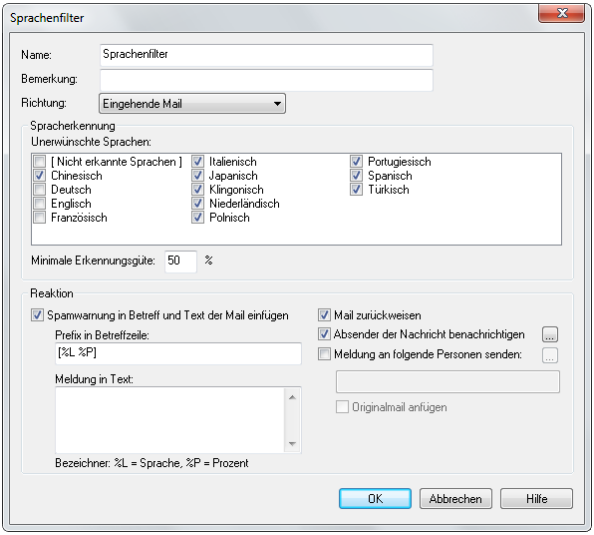


Der Filter kann sowohl im Blacklist- als auch im Whitelist-Modus verwendet werden. Geben Sie unter **Name** und **Bemerkung** Informationen dazu ein, wieso sie die jeweiligen IP-Adressen sperren oder erlauben möchten und dann jede einzelne IP-Adresse unter **IP-Adressen** ein. Klicken Sie auf **Hinzufügen** und die aktuell eingetragene IP-Adresse wird in die Liste der gesperrten IP-Adressen übernommen. Unter Modus können Sie dabei festlegen, ob der IP-Filter im Whitelist-Modus nur bestimmte IP-Adressräume erlauben soll oder im Blacklist-Modus nur bestimmte IP-

Adressräume sperren soll. Sie können die Liste der IP-Adressen auch als txt-Datei exportieren oder eine entsprechende txt-Liste mit IP-Adressen importieren.

9.3.2.11. Sprachenfilter

Mit dem Sprachenfilter können Sie automatisch Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definierung von Englisch als Spam-Sprache sehr viele Spams ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären Mails erhalten und G Data MailSecurity erhöht damit die Spameinschätzung für diese Mails erheblich.

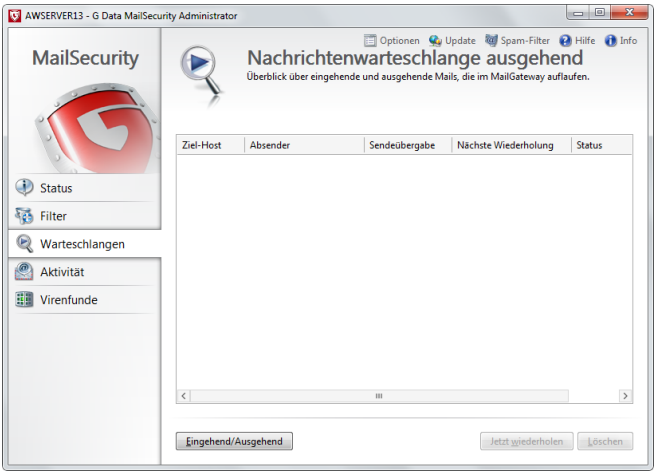


9.3.3. Warteschlangen

Im Warteschlangen-Bereich haben Sie jederzeit Überblick über eingehende und ausgehende Mails, die im MailGateway auflaufen und auf Viren und/oder Content überprüft werden. Die Mails werden in der Regel sofort weitergeleitet, durch das MailGateway nur minimal verzögert und dann auch sofort wieder aus der Warteschlangenliste gelöscht. Sobald eine Mail nicht zustellbar ist oder sich Verzögerungen in der Zustellung ergeben (weil der jeweilige Server z.B. momentan nicht erreichbar ist), erfolgt in der Warteschlangenliste ein entsprechender Eintrag. G Data MailSecurity versucht dann in einstellbaren Abständen (unter **Optionen** > **Warteschlange**) die Mail erneut zu verschicken.

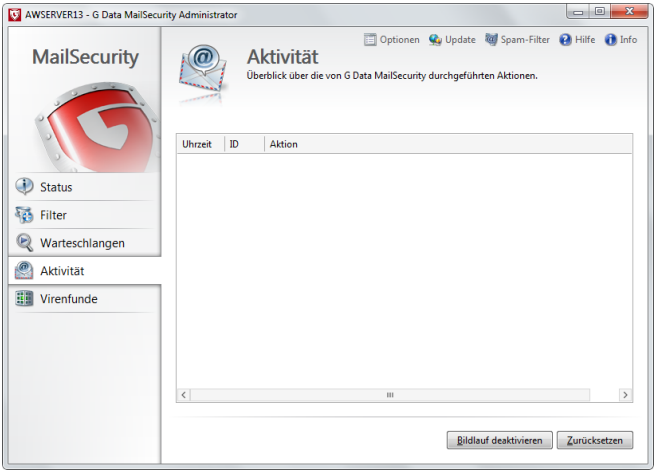
Eine nicht erfolgte oder verzögerte Mailzustellung wird auf diese Weise jederzeit dokumentiert. Über die Schaltfläche **Eingehend/Ausgehend** wechseln Sie von der Listenansicht für eingehende Mails zur Listenansicht für ausgehende Mails. Über die

Schaltfläche **Jetzt wiederholen** können Sie eine markierte Mail, die nicht zugestellt werden konnte - unabhängig von den Zeitvorgaben, die Sie für eine erneute Zustellung unter **Optionen** > **Warteschlange** definiert haben - erneut zustellen. Mit der **Löschen**-Schaltfläche entfernen Sie eine nicht zustellbare Mail endgültig aus der Queue.



9.3.4. Aktivität

Im Aktivität-Bereich haben Sie jederzeit Überblick über die von G Data MailSecurity durchgeführten Aktionen.



Aktionen werden mit **Uhrzeit**, **ID** und **Aktion** in der Aktivität-Liste aufgelistet. Mit dem Scrollbalken rechts können Sie in dem Protokoll auf und abscrollen. Über die **Zurücksetzen**-Schaltfläche löschen Sie das bis dahin erzeugte Protokoll und G Data

MailSecurity beginnt die Aufzeichnung der Aktivitäten erneut. Mit der Funktion **Bildlauf deaktivieren** wird die Liste weiterhin aktualisiert, aber die neuesten Aktivitäten werden nicht direkt an erster Stelle eingeblendet. Sie können dann konzentrierter in der Liste scrollen.

> Über die ID können Sie die protokollierten Aktionen eindeutig einzelnen Mails zuordnen. So gehören Vorgänge mit gleicher ID immer zusammen (z.B. 12345 Lade Mail, 12345 Verarbeite Mail, 12345 Sende Mail).

9.3.5. Virenfunde

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann G Data MailSecurity eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind. Über **Löschen** entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.

10. G Data Internet Security für Android

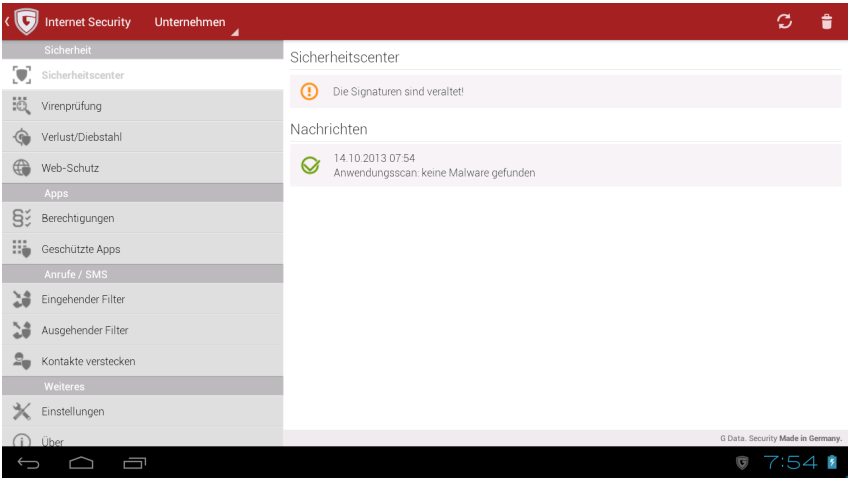
Mit dieser App erhalten Sie eine speziell auf die G Data Netzwerklösung zugeschnittene Version der G Data Internet Security für Android-App und können so Netzwerksicherheit auch über das G Data's Mobile Device Management realisieren. Die Installation der App erfolgt über den **G Data Administrator**.

10.1. Sicherheit

Die Sicherheitsmodule kombinieren alle präventiven Leistungen der Internet Security-App. Sie können über das **Mobile-Einstellungen**-Modul des G Data Administrators zentral gesteuert werden oder manuell konfiguriert und gestartet werden (falls genehmigt).

10.1.1. Sicherheitscenter

Der Sicherheitscenter-Bereich bietet einen Überblick über alle wichtigen Sicherheits-Features. Unter **Sicherheitscenter** finden Sie Warnungen wie Signaturupdate-Erinnerungen. Der Bereich **Nachrichten** erlaubt Ihnen, Einblick in Berichte zu nehmen, wie z.B. Virenprüfungs-Reports oder Reports zum Signatur-Update. Wählen Sie einen Protokolleintrag aus, um sich Details anzeigen zu lassen. Das Erstellen von Protokollen kann im Bereich **Einstellungen** an- oder abgeschaltet werden.

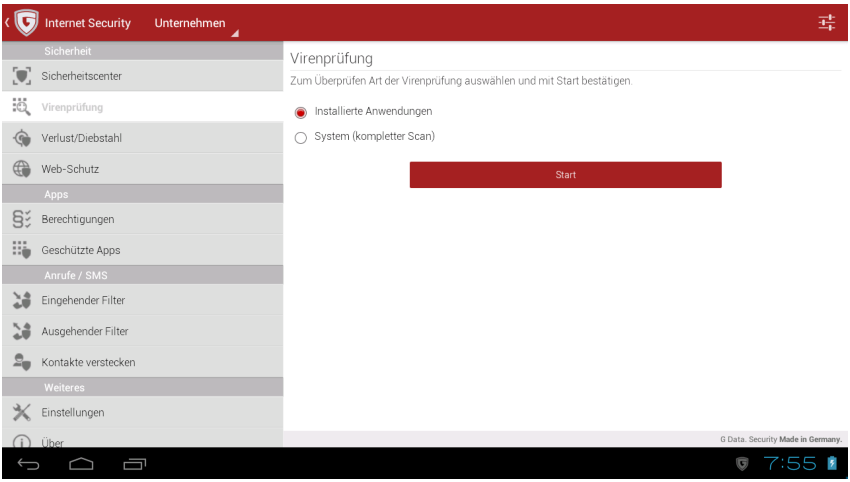


Über die Schaltflächen am oberen rechten Rand des Bildschirms können Sie nach aktuellen Updates für die App suchen und Nachrichten löschen.

10.1.2. Virenprüfung

Wenn Sie unabhängig von der automatischen Prüfung Ihr Gerät manuell überprüfen wollen, wählen Sie dann unter Virenprüfung aus, welche Art der Virenprüfung stattfinden soll und drücken Sie auf Start.

- **Installierte Anwendungen**: Dieser Scan analysiert installierte Anwendungen, um Malware zu identifizieren. Wenn Sie tatsächlich Schadsoftware (Malware) auf Ihrem Gerät haben sollten, haben Sie dann direkt die Möglichkeit, die jeweilige Anwendung zu deinstallieren.
- **System (kompletter Scan)**: Hier wird der gesamte Smartphone-Speicher auf Malware überprüft. Damit können Sie z.B. schädliche Applikationen auf der SD-Karte scannen, bevor Sie überhaupt installiert werden.



Wählen Sie die **Einstellungen**-Schaltfläche oben rechts im Programmfenster, um die **Virenprüfung**-Einstellungen zu öffnen.

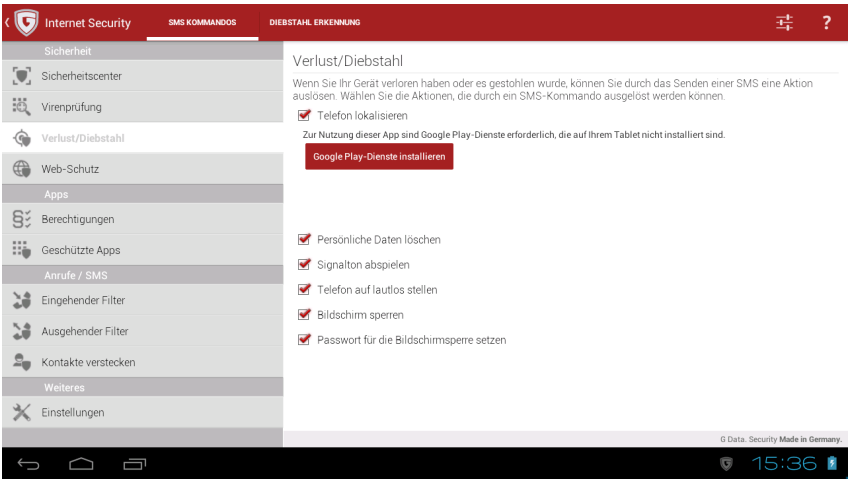
10.1.3. Verlust/Diebstahl

Um verlorene oder gestohlene Mobilgeräte zu schützen, bietet die Internet Security verschiedene Maßnahmen an. Die **SMS Kommandos** erlauben Ihnen, Maßnahmen zu wählen die über SMS aktiviert werden können. **Diebstahl Erkennung** kann verwendet werden, um Methoden die üblicherweise von Dieben genutzt werden zu vereiteln.

Wenn Sie das erste Mal das Menü Verlust/Diebstahl öffnen, werden Sie aufgefordert, ein **Passwort**, Ihre **Telefonnummer** (optional) und **E-Mail-Adresse** (optional) anzugeben. Sollten Sie diese schon vorher über den G Data Administrator unter **Mobile-Einstellungen** definiert haben, ist dies nicht notwendig. Verwenden Sie das Einstellungen-Symbol in der rechten oberen Ecke, wenn die Einstellungen nachher geändert werden müssen.

10.1.3.1. SMS Kommandos

Um verlorene oder gestohlene Geräte zu schützen, bietet Internet Security verschiedene Maßnahmen, die ferngesteuert über SMS aktiviert werden können.



Hier können Sie festlegen, welche Aktionen mit Ihrem Smartphone ausgeführt werden, sobald Sie diesem ein SMS-Kommando zuschicken. Setzen Sie hierzu Häkchen bei den Funktionen, die Sie aktivieren möchten:

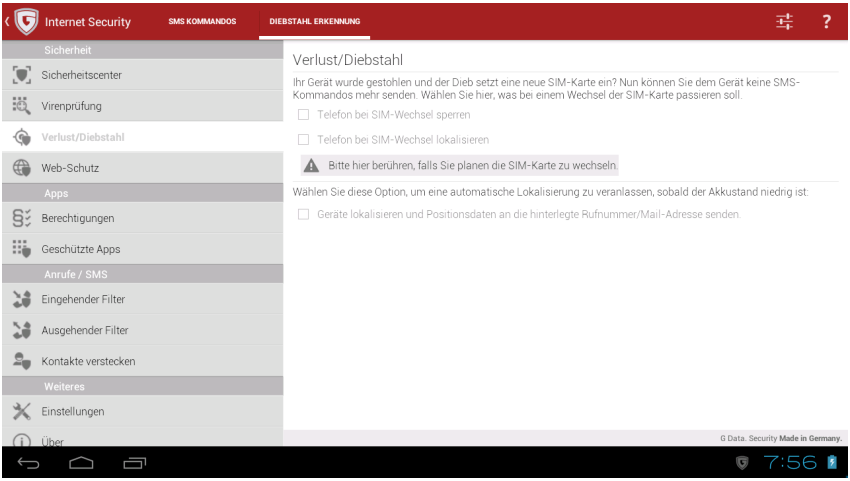
- **Telefon lokalisieren** (auch über die **Mobile-Einstellungen** des Administrators)
- **Persönliche Daten löschen** (auch über die **Mobile-Einstellungen** des Administrators)
- **Signalton abspielen** (auch über die **Mobile-Einstellungen** des Administrators)
- **Telefon auf lautlos stellen** (auch über die **Mobile-Einstellungen** des Administrators)
- **Bildschirm sperren** (auch über die **Mobile-Einstellungen** des Administrators)
- **Passwort für die Bildschirmsperre setzen** (auch über die **Mobile-Einstellungen** des Administrators)

10.1.3.2. Diebstahl Erkennung

Sollte Ihr Smartphone gestohlen worden sein und der Dieb eine neue SIM-Karte einsetzen, so funktionieren die Remote options nicht. Mithilfe von der Diebstahlerkennung, können Sie folgende Aktionen ausführen sobald die SIM-Karte gewechselt wird:

- **Telefon bei SIM-Wechsel sperren** (auch über die **Mobile-Einstellungen** des Administrators)
- **Telefon bei SIM-Wechsel lokalisieren** (auch über die **Mobile-Einstellungen** des Administrators)

Wenn Sie selber die SIM-Karte wechseln möchten, verwenden Sie die Option **Bitte hier berühren, falls Sie planen die SIM-Karte zu wechseln**. Dies deaktiviert vorübergehend die SIM-Erkennung bis das Gerät neu gestartet wird.

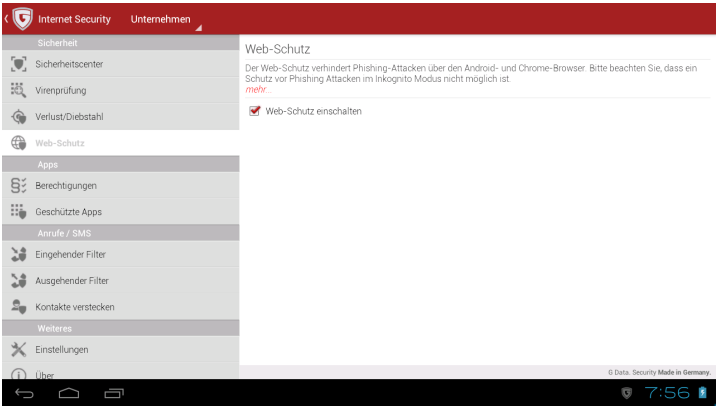

Internet Security
SMS KOMMANDOS
DIEBSTAHL ERKENNUNG
Sicherheit
Sicherheitscenter
Virenprüfung
Verlust/Diebstahl
Web-Schutz
Apps
Berechtigungen
Geschützte Apps
Anrufe / SMS
Eingehender Filter
Ausgehender Filter
Kontakte verstecken
Weiteres
Einstellungen
Über
Verlust/Diebstahl
Ihr Gerät wurde gestohlen und der Dieb setzt eine neue SIM-Karte ein? Nun können Sie dem Gerät keine SMS-Kommandos mehr senden. Wählen Sie hier, was bei einem Wechsel der SIM-Karte passieren soll:
Telefon bei SIM-Wechsel sperren
Telefon bei SIM-Wechsel lokalisieren
Bitte hier berühren, falls Sie planen die SIM-Karte zu wechseln.
Wählen Sie diese Option, um eine automatische Lokalisierung zu veranlassen, sobald der Akkustand niedrig ist:
Geräte lokalisieren und Positionsdaten an die hinterlegte Rufnummer/Mail-Adresse senden.
G Data. Security Made in Germany.
7:56

Wenn das Gerät im Akkusparmodus ist, wird es nicht mehr automatisch seine Position speichern. Wählen Sie **Geräte lokalisieren und Positionsdaten an die hinterlegte Rufnummer/Mail-Adresse senden**, um das Gerät direkt bei der Aktivierung des Akkusparmodus seine letzte bekannte Position melden zu lassen.

10.1.4. Web-Schutz

Das Modul Web-Schutz schützt Sie vor Phishing-Attacken. Es blockt Phishing-Websites, so dass diese auf Ihrem Android-Browser und auf Chrome nicht geöffnet werden können. Da der Web-Schutz immer auch ein gewisses Datenvolumen nach sich zieht, können Sie den Phishing-Schutz im **Einstellungen**-Bereich auch so einstellen, dass er nur dann aktiv ist, wenn Sie mit ihrem Smartphone WLAN nutzen.

Der Web-Schutz kann auch zentral über den Bereich **Mobile-Einstellungen** im G Data Administrator eingestellt werden.

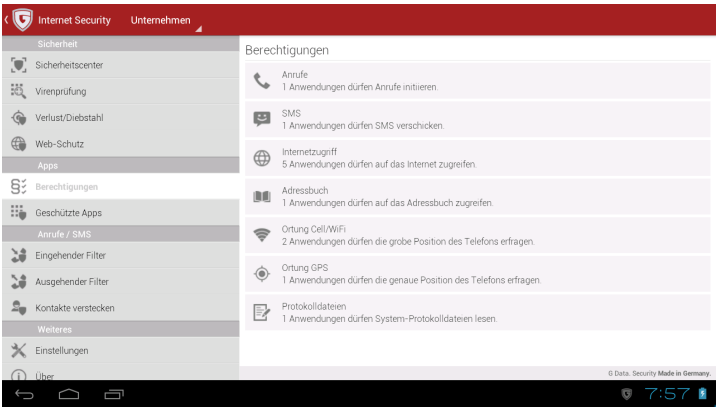


10.2. Apps

Die Module unter Apps ermöglichen die Überwachung der Berechtigungen für installierte Apps und die Blockierung von Apps.

10.2.1. Berechtigungen

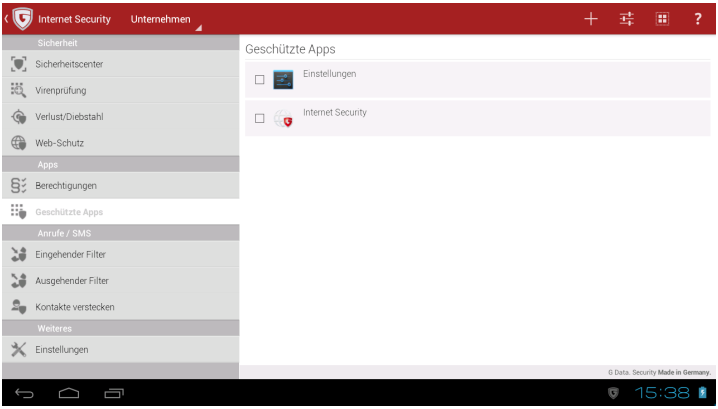
Im Bereich Berechtigungen haben Sie die Möglicheit, sich die Berechtigungen all Ihrer Apps anzeigen zu lassen und dann zu entscheiden, ob Sie eine App nicht vielleicht wieder löschen. Eine kostenlose Spiele-App, die auf das Adressbuch zugreift und SMS verschicken darf, sollte z.B. äußerst kritisch betrachtet werden. Wenn Sie einen Eintrag mit Berechtigungen antippen (z.B. **Anrufe** oder **Internetzugriff**) werden Ihnen alle Apps angezeigt, die diese Berechtigungen haben. Von hier aus können Sie Apps dann auch direkt deinstallieren oder den **Geschützte Apps** hinzufügen.



10.2.2. Geschützte Apps

Über den App-Schutz können Sie bestimmte Apps auf Ihrem Smartphone vor unerlaubtem Zugriff schützen, so können Sie z.B. den Play-Store sperren, damit keine Apps ohne Ihre Erlaubnis gekauft werden. Wenn Sie das erste Mal die App-Schutz-Einstellungen aufrufen, werden Sie dazu aufgefordert, **Passwort**, **E-Mail-Adresse** und eine **Sicherheitsfrage** anzugeben. Sollten Sie diese schon vorher über den G Data Administrator unter **Mobile-Einstellungen** definiert haben, ist dies nicht notwendig.

Wählen Sie **App-Schutz einschalten**, um die Option zu aktivieren. Die Einstellungen können jederzeit durch Antippen des **Einstellungen**-Symbols in der oberen rechten Ecke geändert werden.



In der Hauptansicht des App-Schutz-Moduls sehen Sie eine Liste der geschützten Apps. Tippen Sie hier auf das **+** Symbol in der Titelzeile um die Apps auszuwählen, die Sie schützen möchten. Um eine App mit dem App-Schutz per Passwort zu schützen, setzen Sie einfach ein Häkchen vor die App. Genauso leicht können Sie den Schutz von Apps wieder abschalten, indem Sie das Häkchen vor der jeweiligen App hier entfernen.

10.3. Anrufe / SMS

Der Bereich Anrufe / SMS kombiniert Filtermöglichkeiten mit der Kontakteverwaltung.

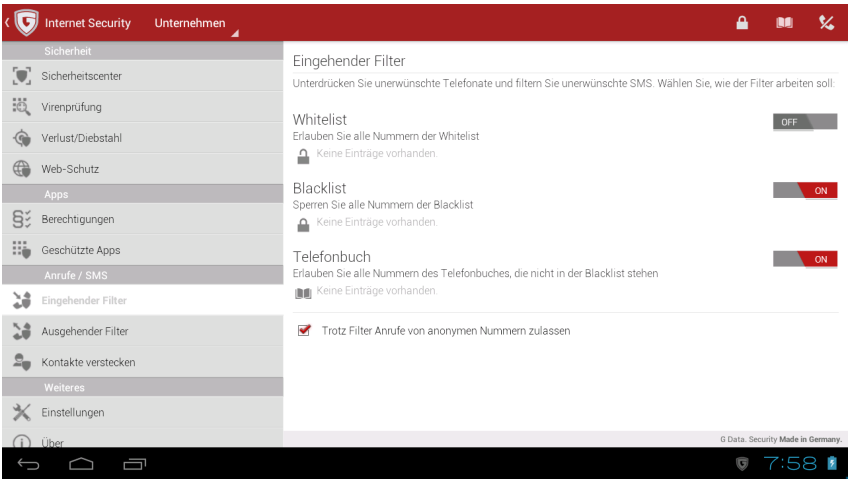
10.3.1. Eingehender Filter

Es gibt zwei Möglichkeiten im Bereich Eingehender Filter bestimmte Absender für Anrufe und SMS zu filtern.

- **Whitelist**: Nur Einträge auf dieser Liste werden durchgestellt
- **Blacklist**: Einträge auf dieser Liste werden unterdrückt

- **Telefonbuch**: Einträge im Telefonbuch werden durchgestellt, wenn sie nicht auf der Blacklist gespeichert wurden.

Die Filterliste Telefonbuch lässt sich mit der White- oder Blacklist kombinieren. Optional können anonyme Anrufe durchgestellt/unterdrückt werden, indem das Häkchen bei **Trotz Filter Anrufe von anonymen Nummern zulassen** gesetzt wird.

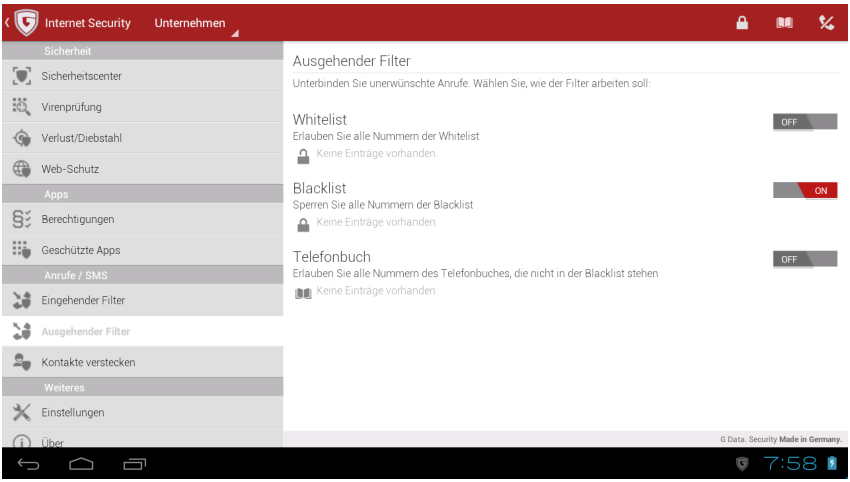


Um Einträge auf der Black- oder Whitelist anzuschauen, tippen Sie auf das Schloss-Icon. Um eine Telefonnummer zur Liste hinzuzufügen, tippen Sie auf das Plus-Icon. Telefonnummern können aus dem Adressbuch oder der Anrufhistorie ausgewählt werden. Bei manueller Eingabe können Sie Platzhalter verwenden, um mehrere Nummern auf einmal zu blockieren (Blacklist) oder erlauben (Whitelist). Der Punkt (.) ist Platzhalter für ein einzelnes Zeichen. Das Sternchen-Symbol (*) ist Platzhalter für ganze Zeichenfolgen. Zum Beispiel: Die Eingabe *0180** entspricht allen Nummern beginnend mit 0180. Die Eingabe *012 345678.* entspricht allen Nummern von 012 3456780 bis 012 3456789, aber nicht 012 34567800. Bei einem eingehenden oder ausgehenden Anruf wird sowohl die nationale (z.B. 012 3456789) als auch die internationale (z.B. 0049 12 3456789) Nummernformatierung ausgewertet. Es gilt als Treffer, wenn entweder eine oder beide der Nummernformatierungen mit der Zeichenfolge inklusive Platzhalter übereinstimmen.

Der Anruf-/SMS-Filter kann auch zentral über den G Data Administrator verwaltet werden (**Mobile-Einstellungen** > **Anruf-Filter**).

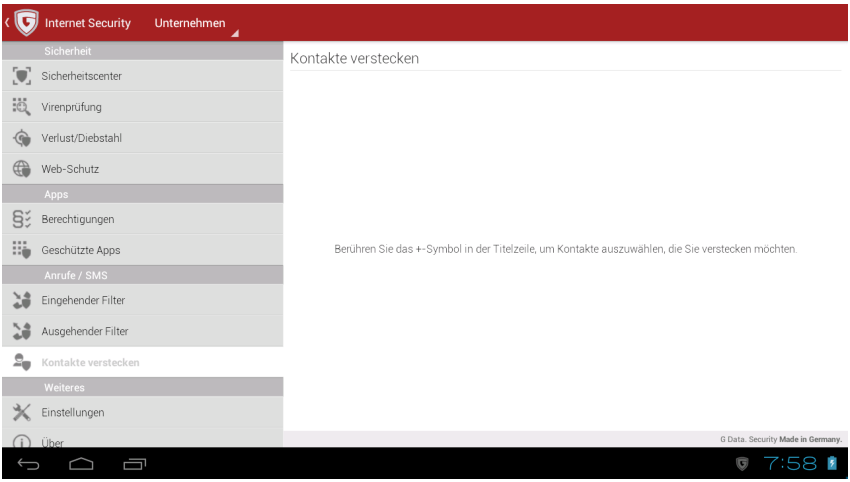
10.3.2. Ausgehender Filter

Der Ausgehende Filter funktioniert ähnlich wie der **Eingehende Filter**, indem Sie eine Black- oder Whitelist für ausgehende Anrufe definieren können.



10.3.3. Kontakte verstecken

Kontakte und ihre eingehenden Anrufe und Nachrichten können verborgen werden. Dazu verschieben Sie den jeweiligen Kontakt in einen geschlossenen G Data-Account im Modul **Kontakte verstecken**. Das erweiterte Kontaktmanagement kann über den G Data Administrator durchgeführt werden (**Mobile-Einstellungen** > **Telefonbuch**).



Wählen Sie die Kontakte verstecken-Option um eine Liste der momentan versteckten Kontakte anzuzeigen. Um einen Kontakt hier hinzuzufügen, tippen Sie bitte auf das Plus-Symbol. Sie können hierzu jeden Kontakt aus Ihrem Adressbuch oder der Telefonhistorie wählen. Nachdem der Kontakt in die Liste aufgenommen wurde, können Sie Einstellungen vornehmen, indem Sie den Namen des Kontaktes antippen. Um eingehende Nachrichten und Anrufe zu verbergen, wählen Sie **Kommunikation**

verbergen. Um einen Kontakt aus dem Adressbuch zu verbergen, wählen Sie **Kontakte verbergen**. Verborgene Nachrichten können über die Auswahl von **Nachrichtenverlauf** oder **Anrufhistorie** angezeigt werden. Um einen Kontakt wieder anzuzeigen, wählen Sie ihn bitte aus und tippen auf **Einträge entfernen**. Der Kontakt wird dann aus dem verborgenen Bereich wieder in Ihr öffentliches Adressbuch übertragen.

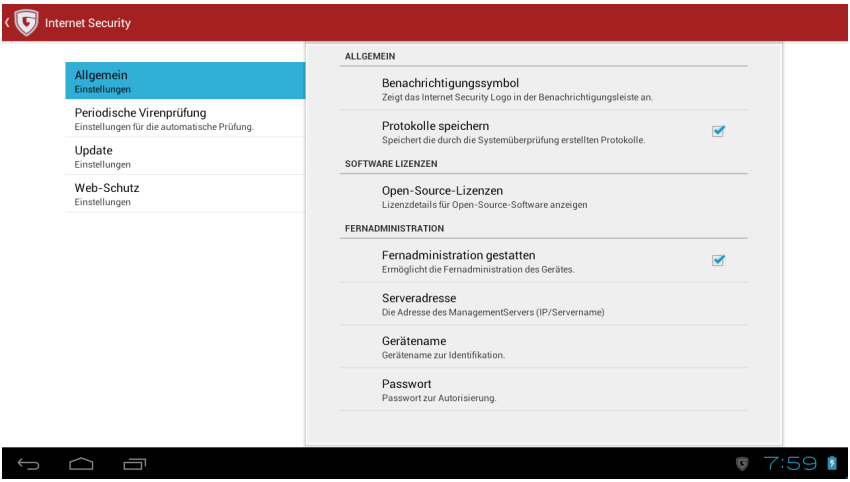
10.4. Einstellungen

Die meisten Einstellungen der G Data Internet Security können direkt über den **Mobile-Einstellungen** Bereich des G Data Administrators durchgeführt werden. Auf dem Mobilgerät haben Sie darüber hinaus auch die Möglichkeit, einige Einstellungen vorzunehmen.

10.4.1. Allgemein

Der Allgemein-Bereich beinhaltet das Tray-Icon und die Scan-Log-Einstellungen.

- **Benachrichtigungssymbol**: Zeigt das Logo der G Data Internet Security in der Benachrichtigungsleiste an.
- **Protokolle speichern**: Speichert die durch die Systemüberprüfung erstellten Protokolle.



Im Abschnitt Fernadministration können Sie Server-Einstellungen konfigurieren, um Geräte ferngesteuert zu administrieren.

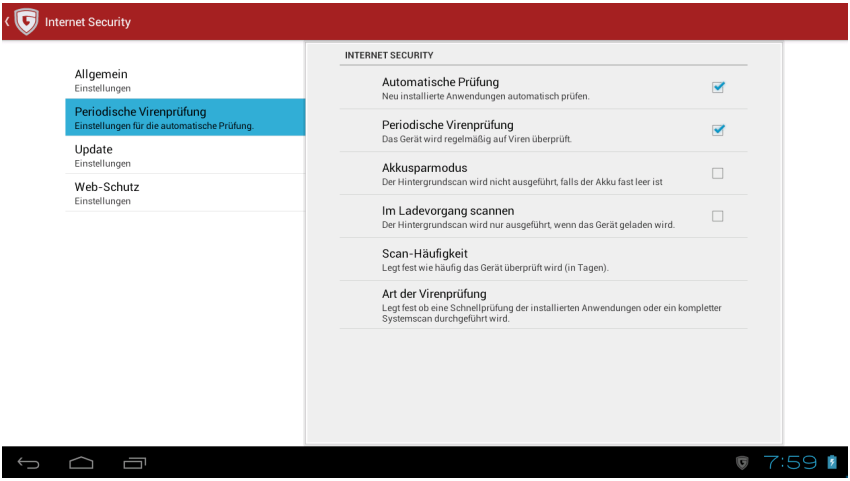
- **Fernadministration gestatten**: Erlaubt Internet Security durch den G Data ManagementServer administriert zu werden.
- **Serveradresse**: Geben Sie hier die IP-Adresse oder den Servernamen des G Data ManagementServers an.

- **Gerätename**: Geben Sie hier den Gerätenamen an.
- **Passwort**: Geben Sie hier das Passwort ein, welches dazu verwendet wird, das mobile Gerät beim G Data ManagementServer zu authentifizieren (das Passwort wird im G Data Administrator im Bereich **Server-Einstellungen** definiert).

10.4.2. Periodische Virenprüfung

Der Abschnitt Periodische Virenprüfung bietet schnellen Zugriff auf die Virus-Scan-Modul-Einstellungen.

- **Automatische Prüfung** (auch über die **Mobile-Einstellungen** des Administrators)
- **Periodische Virenprüfung** (auch über die **Mobile-Einstellungen** des Administrators)
- **Akkusparmodus** (auch über die **Mobile-Einstellungen** des Administrators)
- **Im Ladevorgang scannen** (auch über die **Mobile-Einstellungen** des Administrators)
- **Scan-Häufigkeit** (auch über die **Mobile-Einstellungen** des Administrators)
- **Art der Virenprüfung** (auch über die **Mobile-Einstellungen** des Administrators)

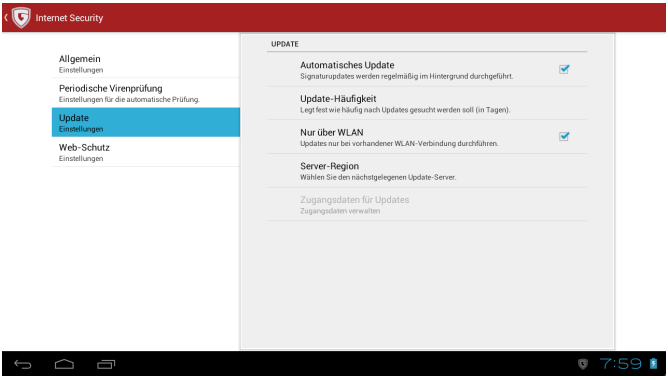


10.4.3. Update

Der Automatisches Update-Bereich umfasst Einstellungen für Updates der Virensignaturen und die Regionsauswahl für den Update-Server.

- **Automatisches Update** (auch über die **Mobile-Einstellungen** des Administrators)

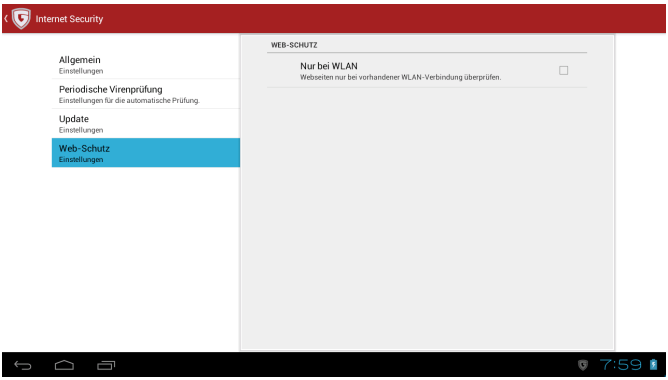
- **Update-Häufigkeit** (auch über die **Mobile-Einstellungen** des Administrators)
- **Nur über WLAN** (auch über die **Mobile-Einstellungen** des Administrators)
- **Server-Region**: Wählen Sie hier den Update-Server aus (nicht aktiv, wenn die Fernadministration aktiviert wurde). Wenn Internet Security das erste Mal Updates anfordert, wird automatisch der nächstliegende Update-Server ausgewählt.



10.4.4. Web-Schutz

Der Web-Schutz-Bereich beinhaltet die Möglichkeit, Web-Schutz auf WLAN-Netze zu begrenzen.

- **Nur bei WLAN** (auch über die **Mobile-Einstellungen** des Administrators)



11. FAQ

11.1. Installation

11.1.1. Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher

Der Wächter überwacht im Hintergrund alle Dateizugriffe und prüft im Zugriff befindliche Dateien auf Viren. Dieses führt normalerweise zu einer kaum spürbaren Verzögerung. Falls eine Anwendung sehr viele Dateien oder einige Dateien sehr oft öffnet, kann eine erhebliche Verzögerung auftreten. Um dies zu umgehen, deaktivieren Sie den Wächter zunächst temporär, um herauszufinden, ob die Verzögerungen durch ihn hervorgerufen werden. Wenn der betroffene Rechner auf Dateien eines Servers zugreift, muss auch der Wächter auf dem Server temporär deaktiviert werden. Falls der Wächter die Ursache ist, kann das Problem i.d.R. durch die Definition einer Ausnahme (Dateien, die nicht geprüft werden sollen) behoben werden. Dazu müssen zunächst die Dateien ermittelt werden, auf die häufig zugegriffen wird. Mit einem Programm wie z.B. MonActivity können diese Daten ermittelt werden. Wenden Sie sich hierzu ggf. an unser **ServiceCenter**.

> Selbstverständlich können Sie auch die Performance dadurch steigern, indem Sie nicht beide Engines zur Virenüberprüfung verwenden, sondern nur eine Engine. Dies bietet sich in erster Linie auf älteren Systemen an und kann im **Wächter**-Bereich eingestellt werden.

11.1.2. Ich habe die G Data Software ohne Registrierung installiert. Wie kann ich die Software registrieren?

Um die Software nachträglich zu registrieren, öffnen Sie unter **Start** > **Alle Programme** > **G Data** > **G Data ManagementServer** das **Internet-Update**. Dort steht die Option **Online-Registrierung** zur Verfügung. Nach einem Klick auf diese Schaltfläche öffnet sich das Registrierungsformular. Geben Sie dort die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgter Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich. Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendetem Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

> Sollten Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder als

Zusatzmodul einen G Data PatchManager erworben und bei der Installation nicht aktiviert haben, werden die Karteireiter Firewall, PatchManager und PolicyManager erst nach erfolgreicher Aktivierung freigeschaltet. Bis dahin stehen nur die Funktionen von G Data AntiVirus Business zur Verfügung.

11.1.3. MailSecurity, Exchange Server 2000 und AVM Ken!

Wenn Sie AVM Ken! nutzen und die G Data MailSecurity auf demselben Computer wie den Ken!-server installieren möchten, wenden Sie sich bitte an unser **Support-Team** für detaillierte Informationen.

Wenn Sie den Exchange Server 2000 nutzen und die G Data MailSecurity auf demselben Computer wie den Exchange Server installieren möchten oder wenn Sie die Ports für ein- und ausgehende Mails auf dem Exchange Server ändern möchten, wenden Sie sich bitte an unser **Support-Team** für detaillierte Informationen.

11.2. Fehlermeldungen

11.2.1. Client: "Programmdateien wurden verändert oder sind beschädigt"

Um einen optimalen Virenschutz zu gewährleisten, werden die Programmdateien regelmäßig auf Ihre Integrität geprüft. Bei einem Fehler wird der Bericht **Programmdateien wurden verändert oder sind beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Programmdateien (G Data Client) von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Programmdateien durch. Kontaktieren Sie unsere **telefonische Hotline**, wenn der Fehlerbericht erneut eingefügt wird.

11.2.2. Client: "Die Virendatenbank ist beschädigt."

Um einen optimalen Virenschutz zu gewährleisten wird die Virendatenbank regelmäßig auf Ihre Unversehrtheit geprüft. Bei einem Fehler wird der Bericht **Die Virendatenbank ist beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Virendatenbank von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Virendatenbank durch. Kontaktieren Sie unsere **telefonische Hotline**, wenn der Fehlerbericht erneut eingefügt wird.

11.2.3. "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1"

Sollten Sie die Fehlermeldung "Zur Installation von G Data MailSecurity benötigen Sie mindestens Microsoft® Exchange Server 2007 SP1" erhalten, sind die Mindestvoraussetzungen für die Installation des G Data MailSecurity Exchange-Plugins nicht erfüllt. Für eine Installation wird mindestens Microsoft Exchange 2007 mit Service

Pack 1 benötigt. Dieser muss vor der G Data MailSecurity installiert werden. Siehe hierzu auch **Installation** und **Systemvoraussetzungen**.

11.3. Linux

11.3.1. Linux-Fileserver Clients: Es wird keine Verbindung zum G Data ManagementServer aufgebaut / Signaturen werden nicht aktualisiert

Falls einige Linux-Fileserver-Clients keine Verbindung zum G Data ManagementServer aufbauen oder Signaturen nicht aktualisiert werden, führen Sie folgende Schritte durch:

1. Prüfen Sie ob die beiden Prozesse des G Data Linux-Clients laufen. Geben Sie im Terminal:

   linux:~# *ps ax|grep av*

   ein. Sie sollte die Ausgaben

   Ssl 0:07 /usr/sbin/avkserver --daemon
   Ssl 0:05 /usr/sbin/avclient --daemon

   erhalten. Sie können die Prozesse unabhängig von der eingesetzten Distribution mit

   linux:~# */etc/init.d/avkserver start*
   linux:~# */etc/init.d/avclient start*

   starten und mit

   linux:~# */etc/init.d/avkserver stop*
   linux:~# */etc/init.d/avclient stop*

   anhalten. Hierzu müssen Sie als Administrator (root) auf dem Linux-Rechner eingeloggt sein.
2. Sehen Sie sich die Log-Dateien an: Unter /var/log/ befindet sich die Log-Datei gdata_install.log. In dieser Datei wird der Verlauf der Remote-Installation protokolliert. Im Verzeichnis /var/log/gdata befindet sich die Log-Datei avkclient.log. In dieser Log-Datei werden die Scan-Ergebnisse des Scanners avkserver und die Ausgaben des Prozesses avclient protokolliert, der die Verbindung zum G Data ManagementServer herstellt. Schauen Sie sich die Dateien an und suchen Sie nach Fehlermeldungen. Wenn Sie mehr Meldungen sehen möchten, können Sie in den Konfigurationsdateien /etc/gdata/gdav.ini und etc/gdata/avclient.cfg die Einträge für **LogLevel** auf den Wert *7* setzen.

   Vorsicht: Hohe LogLevel erzeugen viele Meldungen und lassen die Log-Dateien schnell anwachsen. Setzen Sie die LogLevel im Normalbetrieb

immer auf niedrige Werte.

3. Testen Sie den Scanner: Mit dem Kommandozeilen-Tool avkclient können sie die Funktion des Scanservers avkserver testen. Folgende Kommandos lassen sich ausführen:

   linux:~$ *avkclient avkversion* - gibt Version und Updatedatum der Virensignaturen aus
   linux:~$ *avkclient version* - gibt Version in Kurzform aus
   linux:~$ *avkclient scan:<file>* - scannt die Datei <file> und gibt das Ergebnis aus

4. Sehen Sie sich die Konfigurationsdatei an: Unter etc/gdata/avclient.cfg finden Sie die Konfigurationsdatei des Remoteclients avclient. Kontrollieren Sie, ob die Adresse des Haupt-Management-Servers (MainMMS) korrekt eingetragen ist. Falls nicht, löschen Sie den falschen Eintrag und melden den Linux-Client über den G Data Administrator erneut an oder tragen Sie die Adresse des G Data ManagementServers direkt ein.

5. Testen Sie Ihre Freigaben: Der Virenschutz für die Samba-Freigaben wird durch den Eintrag *vfs objects = gdvfs* in der Samba-Konfigurationsdatei /etc/samba/smb.conf aktiviert. Steht der Eintrag in der Sektion [global], so ist der Schutz für alle Freigaben aktiviert. Steht die Zeile in einer anderen Sektion, so gilt der Schutz nur für die entsprechende Freigabe. Sie können die Zeile testweise auskommentieren (eine Raute (*#*) voranstellen), um festzustellen, ob der Zugriff ohne den Virenschutz funktioniert. Falls nicht, suchen Sie zunächst den Fehler in Ihrer Samba-Konfiguration.

6. Linux Workstation Wächter: Prüfen Sie, ob der Wächter-Prozess avguard läuft:

   linux:~# *ps ax|grep avguard*

   Der Wächter benötigt die Kernel-Module redirfs und avflt. Sie können mit lsmod prüfen, ob die Module geladen sind: *lsmod|grep redirfs* und *lsmod| grep avflt*.

   Die Module müssen für den von Ihnen verwendeten Kernel kompiliert sein. Dies erledigt das Dynamic Kernel Module System (DKMS), welches zusammen mit den passenden Kernel-Header-Paketen Ihrer Distribution installiert sein muss. Wenn das der Fall ist, kompiliert und installiert DKMS die Module automatisch. Sie finden die Logdatei des Wächters unter /var/log/gdata/avguard.log.

11.4. Sonstiges

11.4.1. Wie kann ich überprüfen, ob die Clients eine Verbindung zum G Data ManagementServer haben?

Die Spalte **Letzter Zugriff** im Aufgabenbereich **Clients** enthält den Zeitpunkt, an dem sich der Client zum letzten Mal beim G Data ManagementServer gemeldet hat. In der Standardeinstellung melden sich die Clients alle fünf Minuten beim G Data ManagementServer (wenn gerade keine Scanaufträge ausgeführt werden). Folgende

Ursachen können für eine fehlgeschlagene Verbindung verantwortlich sein:

- Der Client ist ausgeschaltet oder vom Netzwerk getrennt.
- Es kann keine TCP/IP-Verbindung zwischen dem Client und dem G Data ManagementServer aufgebaut werden. Prüfen Sie die Netzwerkeinstellungen bzw. Portfreigaben.
- Der Client kann die IP-Adresse des Servers nicht ermitteln, d.h. die DNS Namensauflösung funktioniert nicht. Die Verbindung kann mit dem Befehl telnet über die Eingabeaufforderung überprüft werden. Am Server muss TCP Port 7161 erreichbar sein, am Client muss TCP Port 7167 bzw. TCP Port 7169 erreichbar sein. Prüfen Sie die Verbindung mit dem Befehl *telnet <SERVERNAME> <PORTNUMMER>*

  Beachten Sie, dass unter Windows Vista, Windows 7 sowie Server 2008 (R2) der telnet-Befehl standardmäßig nicht verfügbar ist. Aktivieren Sie daher die entpsrechende Windows-Funktion bzw. fügen Sie sie als neues Feature zum Server hinzu. Ist die Verbindung vom Client zum Server intakt, erscheint in der Eingabeaufforderung eine Sammlung kryptischer Zeichen. Wenn die Verbindung vom Server zum Client intakt ist, erscheint ein leeres Eingabefenster.

11.4.2. Mein Postfach wurde in die Quarantäne geschoben

Dies passiert, wenn sich in dem Postfach eine infizierte Mail befindet. Zurückbewegen der Datei: Schließen Sie das Mailprogramm auf dem betroffenen Client und löschen Sie eine evt. neu angelegte Archivdatei. Öffnen Sie anschließend im G Data Administrator den zugehörigen Bericht und klicken Sie auf **Quarantäne: Zurückbewegen**. Kontaktieren Sie bitte unseren **Support**, wenn das Zurückbewegen fehlschlägt.

11.4.3. Mit MMS über IP verbinden

Bei der Installation wird nach dem Servernamen gefragt. Der Name muss durch die IP-Adresse ersetzt werden. Sie können den Servernamen auch nachträglich durch die IP-Adresse ersetzen, wenn der G Data ManagementServer bereits installiert ist. Passen Sie dazu - je nach Ihrem System - einen dieser Registry-Einträge an:

HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVK ManagementServer\ComputerName

Damit die Verbindung vom Server zu den Clients auch über die IP-Adresse hergestellt werden kann, müssen die Clients im G Data Administrator mit Ihrer IP-Adresse aktiviert werden. Das geht entweder von Hand oder durch **Active Directory Synchronization**. Wenn die Clients direkt von dem Installationsmedium installiert werden, fragt das Installationsprogramm sowohl nach dem Servernamen als auch nach dem Computernamen. Geben Sie hier jeweils die IP-Adresse ein.

11.4.4. Speicherorte und Pfade

Virensignaturen G Data Security Client

- Windows XP/Server 2003/Server 2003 R2: C:\Programme\Gemeinsame Dateien \G DATA\AVKScanP\BD bzw. G Data
- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\Programme (x86)\Common Files\G DATA\AVKScanP\BD bzw. G Data

Virensignaturen G Data ManagementServer

- Windows XP/Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Updates
- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data Security Client-Quarantäne

- Windows XP/Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G Data\AntiVirusKit Client\Quarantine
- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\ProgramData\G Data\AntiVirusKit Client\Quarantine

G Data ManagementServer-Quarantäne

- Windows XP/Server 2003/Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

MMS-Datenbanken:

Windows XP/Windows Vista/Windows 7/Windows 8/Server 2003/Server 2003 R2/Server 2008/Server 2008 R2/Server 2012:

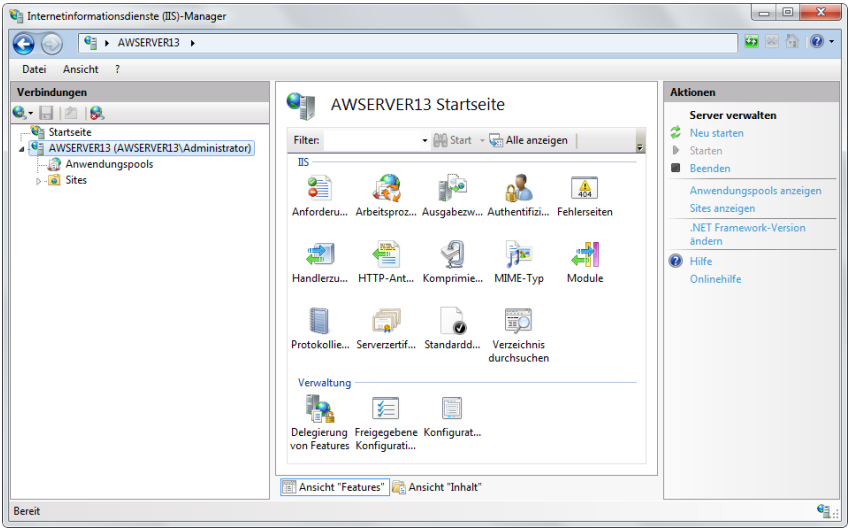
- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data \GDATA_AntiVirus_ManagementServer.mdf
- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log.ldf

11.4.5. Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 7 oder 7.5?

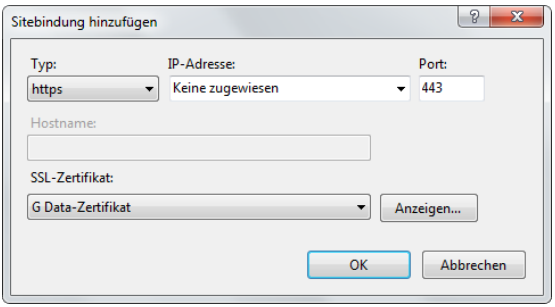
Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.

Um ein SSL-Server-Zertifikat in IIS 7 oder 7.5 zu aktivieren, öffnen Sie bitte **Internetinformationsdienste (IIS)-Manager**. Wenn Sie Windows Server 2008

nutzen, können Sie den IIS Manager unter **Start** > **Alle Programme** > **Verwaltung** finden. Alternativ klicken Sie auf **Start** > **Ausführen** und geben Sie das Kommando *inetmgr* ein. Dieses Kommando kann auch auf Windows 7-Rechnern verwendet werden.



Wählen Sie Ihren Server unter **Verbindungen** aus. Wählen Sie dann die **IIS** Kategorie aus und doppelklicken auf **Serverzertifikate**. Klicken Sie nun auf **Selbstsigniertes Zertifikat erstellen**. Nach der Eingabe eines Namens für das Zertifikat wird dieses erzeugt und in der Serverzertifikat-Übersicht angezeigt. Bitte beachten Sie, dass das Standard-Ablaufdatum für das Zertifikat tagesgenau ein Jahr beträgt.

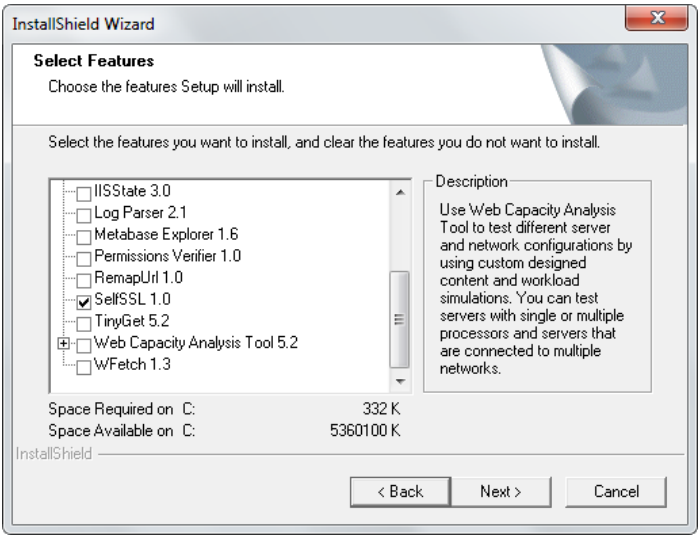


Um das Zertifkat für die Kommunikation zu verwenden wählen Sie die entsprechende Seite im Bereich **Verbindungen** aus. Im Bereich **Aktionen** auf der rechten Seite können Sie nun **Bindungen** auswählen. Klicken Sie nun auf **Hinzufügen**, um eine neue Bindung zu etablieren. Als **Typ** wählen Sie bitte https im DropDown-Menü aus und unter **SSL-Zertifikat** das Zertifikat, welches Sie zuvor definiert haben. Klicken Sie auf **OK**, um die Bindung zu bestätigen.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://* in Ihrem Browser durch *https://* ersetzen, z.B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

11.4.6. Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 5 oder 6?

Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.


InstallShield Wizard
Select Features
Choose the features Setup will install.
Select the features you want to install, and clear the features you do not want to install.
IISState 3.0
Log Parser 2.1
Metabase Explorer 1.6
Permissions Verifier 1.0
RemapUrl 1.0
SelfSSL 1.0
TinyGet 5.2
Web Capacity Analysis Tool 5.2
WFetch 1.3
Description
Use Web Capacity Analysis Tool to test different server and network configurations by using custom designed content and workload simulations. You can test servers with single or multiple processors and servers that are connected to multiple networks.
Space Required on C: 332 K
Space Available on C: 5360100 K
InstallShield
< Back
Next >
Cancel

Um ein SSL-Server-Zertifikat in IIS 5 (Windows XP) oder IIS 6 (Windows Server 2003) zu aktivieren, verwenden Sie bitte das Microsoft-Tool SelfSSL, welches Sie bei den IIS 6.0 Resource Kit Tools (ein kostenloser Download von der Microsoft website) finden. Wenn Sie hier den Setup-Typ **Custom** durchführen, können Sie die Tools auswählen, die Sie installieren möchten. Wählen Sie hier bitte **SelfSSL 1.0** aus. Nach der Installation öffnen Sie die SelfSSL Kommandozeile über **Start** > **Programme** > **IIS Resources** > **SelfSSL**.

Mit Hilfe einer einzigen Eingabe können Sie nun ein selbst signiertes Zertifikat für Ihre Website erzeugen. Geben Sie bitte *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T* ein und drücken Sie dann **Enter**. Bestätigen Sie die Erzeugung des Zertifikats durch Drücken der **Y**-Taste. Nun wird ein Zertifikat für die Standard-IIS Seite auf Ihrem lokalen Server erzeugt und der localhost wird auf die Liste der vertrauenswürdigen Zertifikate hinzugefügt. Die Schlüssellänge beträgt 2048 Zeichen und ist für genau 365 Tage gültig. Wenn Ihre Seite nicht die Standard-ISS Seite auf Ihrem lokalen Server ist, können

Sie unter **Start** > **Programme** > **Verwaltung** > **Internetinformationsdienste (IIS)-Manager** die entsprechende Seite auf Ihrem Server ermitteln und den Parameter */S:1* entsprechend modifizieren.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://* in Ihrem Browser durch *https://* ersetzen, z.B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

12. Lizenzen

SharpSerializer

SharpSerializer is distributed under the New BSD License (BSD). Copyright © 2011, Pawel Idzikowski. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Polenter - Software Solutions nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Json.NET

Json.NET is distributed under The MIT License (MIT). Copyright © 2007 James Newton-King.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip

DotNetZip is distributed under the Microsoft Public License (Ms-PL).

This license governs use of the accompanying software. If you use the software, you accept this license.

If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any

other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index

A
Active Directory 45
Alarmmeldungen 36
Anruf-Filter 81
AntiSpam 71
Anwendungskontrolle 94
App-Schutz 174
Aufträge 82

B
Backupauftrag 88
Backup-Einstellungen 40
BankGuard 71
Benutzerverwaltung 30
Berichte 107
Boot-CD 10

C
Clientauswahlbereich 43
Client-Einstellungen 60
Clients 51
Computer suchen 47

D
Dashboard 50
Deaktivierte Clients 46
Diebstahlschutz 77

E
E-Mail-Einstellungen 38
E-Mail-Schutz 67
Eulas 55

F
Firewall 98

G
G Data Administrator 26
G Data Business 3
G Data ManagementServer 25
Gerätekontrolle 95
Greylist-Filter 155
Gruppe bearbeiten 46

H
Hardware-Inventar 57

I
Installation 6
Installationspaket 20
Installationspaket erstellen 48
Installationsübersicht 48
Internet Security für Android 169
Internetnutzungszeit 97
Internet-Update 32

K
Kontakte verstecken 176

L
Lastbegrenzung 40
Linux-Clients 20
Lizenzmanagement 43
Lokale Installation 20
Lösungen 3

M
MailSecurity Administrator 134
MailSecurity MailGateway 133
MobileAdministrator 116
Mobile-Einstellungen 42, 74

N
Nachrichten 59
Neue Gruppe 46

O
Outlook-Schutz 69

P
PatchManager 104
PolicyManager 93
Port-Konfiguration 9
Port-Überwachung 69
PremiumHotline 5
Programmdateien 34
Programm-Updates 41
Protokoll 29

R
Realtime Blacklists 162
Regelassistent 103
Regelsätze 100
Remote-Installation 18
ReportManager 111

S
Scanauftrag 85
Security Client 121
Security Client deinstallieren 54
Security Client installieren 54
Security Labs 4
Server verwalten 31
Server-Einrichtungsassistent 28
Server-Einstellungen 37
Sicherheitscenter 169
Softwareerkennungsauftrag 91
Software-Inventar 56
Softwareverteilungsauftrag 92
Statistik 113
Subnet-Server-Synchronisation 32
Synchronisation 39
Systemvoraussetzungen 8

U
Update-Rollback 36

V
Verhaltensüberwachung 66
Verlust/Diebstahl 170
Virendatenbank 32

W
Wächter 63
Web/IM 69
WebAdministrator 114
Web-Inhaltskontrolle 96
Wiederherstellungsauftrag 90

Z
Zugangsdaten 35